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

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

November 15, 2023

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

SUBJECT: Fiscal Year 2023 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) 2023. 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 2023 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, six 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 2023 information security program was deemed not-effective because the tested, calculated and assessed maturity levels across the functional and domain areas received an overall rating of Level 3 – Consistently Implemented.

The evaluators identified two new findings with two corresponding recommendations. The two findings are as follows:

1. The agency has not had a risk assessment using the latest controls contained within NIST 800-53 Revision 5.
2. There is no Privacy Policy.

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

cc: Chai Feldblum
Vice-Chairperson
U.S. AbilityOne Commission

Kelvin R. Wood
Chief of Staff
U.S. AbilityOne Commission

Office of Inspector General

for

U.S. AbilityOne Commission

FY 2023 Evaluation of the U.S. AbilityOne Commission's Compliance with the Federal Information Security Modernization Act

September 27, 2023

McConnell Jones
Diverse Thinking | Unique Perspectives

McConnell
Jones

September 27, 2023

Stefania Pozzi Porter
Inspector General
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 2023 (FY23). 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 *FY2023-2024 Inspector General FISMA Reporting Metrics*, Inspectors General are required to assess the effectiveness of information security programs on a maturity model spectrum.

During FY23, there were 2 findings identified with 2 corresponding recommendations regarding the Commission's information security program which included:

1. The agency has not had a risk assessment using the latest controls contained within NIST 800-53 Revision 5.
2. There is no Privacy Policy.

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 2023 information security program was deemed not-effective because the tested, calculated and assessed maturity levels across the functional and domain areas received an overall rating of Level 3 – Consistently Implemented. 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 6 open prior year recommendations from FY20 through FY22. We identified 2 new recommendations during the FY23 evaluation which are detailed within our report. The Commission's comments are included in **Attachment A**.

McConnell
Jones

McConnell & Jones would like to thank the Office of 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

McConnell & Jones LLP

Table of Contents

SECTION **PAGE NUMBER**

Executive Summary

Pursuant to the Federal Information Security 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 FY23 IG FISMA Reporting Metrics. The Commission OIG submitted the cyber metrics into CyberScope on July 26, 2023.

Under *FY 2023-2024 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 an 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 FY23 information security program was deemed not-effective because the tested, calculated and assessed maturity levels across the functional and domain areas received a rating of Level 3 – Consistently Implemented. The table below summarizes the function and maturity level ratings for FY23 FISMA Metrics, as well as the overall rating from the CyberScope system.

Function	Assessed Maturity Level
Function 1: Identify – Risk Management / Supply Chain Risk Management	2 - Defined
Function 2: Protect – Configuration Management / Identity & Access Management / Data Protection & Privacy / Security Training	3 - Consistently Implemented
Function 3: Detect – ISCM	2 - Defined
Function 4: Respond – Incident Response	3 - Consistently Implemented
Function 5: Recover – Contingency Planning	3 - Consistently Implemented
Overall	Not Effective

Our findings and recommendations will improve the Commission's IT security and privacy operations and its compliance with FISMA functional areas.

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 2023-2024 Inspector General FISMA Reporting Metrics*, and the evaluation guide that provides test objectives and procedures.

On December 17, 2002, Congress enacted the E-Government Act of 2002 (Public Law 107-347). 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 August 1, 2022, through July 31, 2023 (FY23).

For purposes of the FY23 FISMA evaluation, we reviewed 19 control families and 87 associated controls. The scope of our testing included the following new controls, along with testing of the controls from the prior year.

Controls noted with an asterisk ("*") are new controls for FY23, and all other controls are repeated controls from FY22 per the NIST 800-53 guidance.

FY23 Controls Tested	
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-8*	System Use Notification
AC-11*	Device Lock
AC-12*	Session Termination
AC-17	Remote Access
AC-19*	Access Controls for Mobile Devices
AC-21*	Information Sharing
Awareness and Training	
AT-1*	Policy and Procedures
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-1*	Policy and Procedures
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-2*	Baseline Configuration
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-1*	Policy and Procedures
CP-2	Contingency Plan
CP-3	Contingency Training
CP-4	Contingency Plan Testing

FY23 Controls Tested	
Control Number	**Control Name**
Identification and Authentication	
IA-1*	Policy and Procedures
IA-2	Identification and Authentication
IA-4	Identifier Management
IA-5	Authenticator Management
IA-7*	Cryptographic Module Authentication
IA-8	Identification and Authentication (Non-Organizational Users)
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
PL-4*	Rules of Behavior
Program Management	
PM-4*	Plan of Action and Milestone Process
PM-5	System Inventory
PM-5(1)*	System Inventory/Inventory of PII
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-20*	Dissemination of Privacy Program Information
PM-27*	Privacy Reporting
PM-30*	Supply Chain Risk Management Strategy
PM-31	Continuous Monitoring Strategy
Personnel Security	
PS-1*	Policy and Procedures
PS-6*	Access Agreements
Privacy	
PT-5*	Privacy Notice
PT-6*	System of Records Notice

FY23 Controls Tested	
Control Number	**Control Name**
Risk Assessment	
RA-1*	Policy and Procedures
RA-3	Risk Assessment
RA-5	Vulnerability Monitoring and Scanning
RA-5(11)*	Vulnerability Monitoring and Scanning/Penetration Testing and Analysis
RA-8*	Privacy Impact Assessment
RA-9	Criticality Analysis
System and Services Acquisition	
SA-4	Acquisition Process
SA-8(33)*	Security and Privacy Engineering Principles/Minimization
Systems and Communications Protection	
SC-7(10)*	Boundary Protection/Prevent Exfiltration
SC-8	Transmission Confidentiality and Integrity
SC-10*	Network Disconnect
SC-13*	Cryptographic Protection
SC-18	Mobile Code
SC-28	Protection of Information at Rest
System and Information Integrity	
SI-2	Flaw Remediation
SI-3	Malicious Code Protection
SI-4	System Monitoring
SI-4(4)*	System Monitoring/Inbound and Outbound Communications Traffic
SI-4(18)*	System Monitoring/Analyze Traffic and Convert Exfiltration
SI-7(8)*	Software, Firmware, and Information Integrity/Auditing Capability for Significant Events
SI-12(1)*	Information Management and Retention/Limit PII Elements
SI-12(3)*	Information Management and Retention/Information Disposal
Supply Chain Risk Management	
SR-1*	Policy and Procedures
SR-2*	Supply Chain Risk Management Plan
SR-3	Supply Chain Controls and Processes
SR-5	Acquisition Strategies, Tools, and Methods
SR-6	Supplier Assessments and Reviews

**New controls added and tested during the FY23 FISMA audit per NIST800-53 guidance.*

Summary of FY23 Controls Tested	
Control Family	***Number of Controls Tested***
Access Controls (AC)	10
Awareness and Training (AT)	3
Audit and Accountability (AU)	3
Certification, Accreditation and Security Assessments (CA)	6
Configuration Management (CM)	7
Contingency Planning (CP)	4
Identification and Authentication (IA)	6
Incident Response (IR)	3
Media Protection (MP)	2
Personnel Security (PS)	2
Physical and Environmental Protection (PE)	1
Planning (PL)	2
Privacy (PT)	2
Program Management (PM)	12
Risk Assessment (RA)	3
System and Services Acquisition (SA)	2
System Communication Protection (SC)	6
System and Information Integrity (SI)	8
Supply Chain Risk Management (SR)	5
Total Number of Controls Tested	**87**

Current Year Findings

The results of our FY23 FISMA evaluation identified two findings related to the FISMA controls evaluated, and we provide two associated recommendations as noted below.

1. Risk Assessment Deficiency

Condition:
The Commission hasn't completed a risk assessment in accordance with the controls contained within NIST 800-53 Revision 5.

Criteria:
NIST SP 800-53 Revision 5, RA-3 states:
"Control:

a. Conduct a risk assessment, including:

1. Identifying threats to and vulnerabilities in the system;

2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and

3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;

b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;

c. Document risk assessment results in [*Selection: security and privacy plans; risk assessment report;* [*Assignment: organization-defined document*]];

d. Review risk assessment results [*Assignment: organization-defined frequency*];

e. Disseminate risk assessment results to [*Assignment: organization-defined personnel or roles*]; and

f. Update the risk assessment [*Assignment: organization-defined frequency*] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system."

Cause:
Lack of personnel, budget and/or time constraints to adequately document and/or assess all of the controls in NIST SP 800-53.

Risk:
Without completing a risk assessment (at least annually), the agency will be unaware of vulnerabilities that can be exploited and cause harm to the agency.

Recommendation(s):

1. The Commission should implement and undergo an annual Risk Assessment utilizing the latest NIST documents.

Management's Response:

The Commission concurred with the finding and recommendation. Management's comments are included in **Attachment A**, which details the Commission's response regarding not completing a risk assessment.

Auditor's Response to Management's Comments:

Finding 01, Recommendation 1

The Commission is responsible for conducting a periodic risk assessment. Management has issued a procurement to acquire contractual services to perform the required risk assessment, and the expected remediation is estimated to be completed by March 31, 2024. The OIG and Auditors will review and evaluate the subject risk assessment in future evaluations.

2. Privacy Policy Deficiency

Condition:
The Commission has not implemented a privacy policy or program.

Criteria:
NIST SP 800-53 Revision 5, PT-6 states:
"Control:

For systems that process information that will be maintained in a Privacy Act system of records:

a. Draft system of records notices in accordance with OMB guidance and submit new and significantly modified system of records notices to the OMB and appropriate congressional committees for advance review;
b. Publish system of records notices in the Federal Register; and

c. Keep system of records notices accurate, up-to-date, and scoped in accordance with policy."

Cause:
Lack of personnel, budget and/or time constraints to adequately document and/or assess all of the controls in NIST SP 800-53.

Risk:
Without a privacy policy, there is the increased risk that there will be a breach containing Personally Identifiable Information (PII).

Recommendation(s):

1. The Commission should develop a privacy policy in accordance with the privacy related controls contained within NIST 800-53, Revision 5.

Management's Response:

The Commission concurred with the finding and recommendation. Management's comments are included in **Attachment A**, which details the Commission's response regarding the lack of implementation of a privacy policy.

Auditor's Response to Management's Comments:

Finding 02, Recommendation 1

The Commission is responsible for the design and implementation of a privacy policy. Management has stated that such a policy has not been implemented, and the target implementation will be completed by March 31, 2024. The OIG and Auditors will review and evaluate the new policy in future evaluations.

Prior Year Findings

During the FY23 engagement, we reviewed the corrective action status of the findings and recommendations from the FY20 through FY23 evaluations. The results of our evaluation revealed that these recommendations remain open, and implementation of associated remediation actions were not completed as of the July 31, 2023, which is the end of the FY23 FISMA evaluation period.

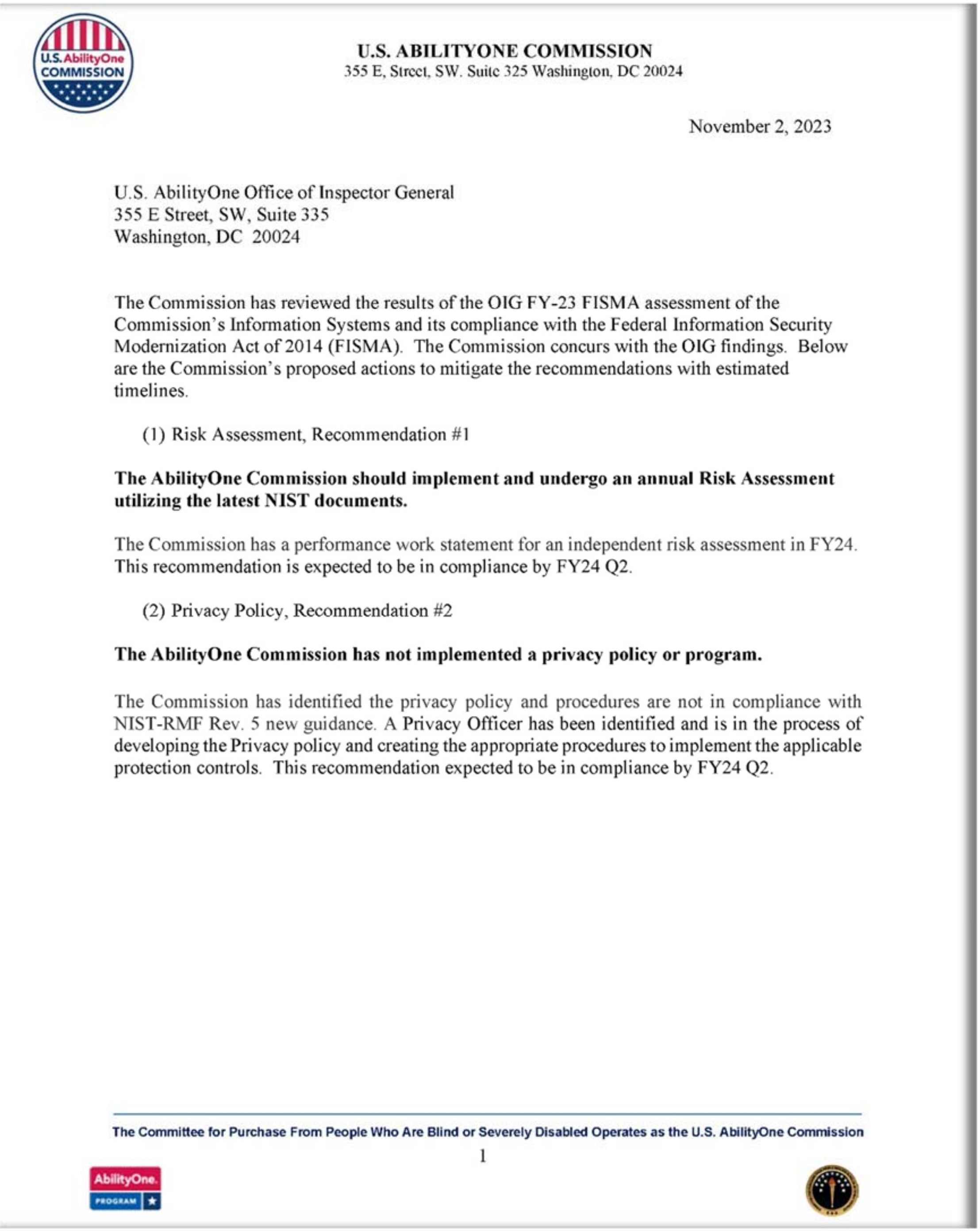
The table below details the status of the prior years' open recommendations:

STATUS OF PRIOR YEARS FISMA RECOMMENDATIONS

Status of Recommendations	Year / Rec. #	Status
The Commission should follow their vulnerability remediation policies (RA-5). 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 (CA-2, CA-5).	2020-1 2020-2	Open
Vulnerabilities not being remediated in a timely manner. (Repeat of finding 2020-1, Recommendation No. 1, RA-5)	2021-1	Open
Configuration settings are not in compliance with Commission policies. (CM-6, CM-7)	2021-2	Open
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. (SR-3)	2022-1	Open
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. (SC-28)	2022-2	Closed
Review and update the Incident Response Plan annually. (I-8)	2022-3	Closed
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. (CP-2)	2022-4	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
355 E, Street, SW. Suite 325 Washington, DC 20024

November 2, 2023

U.S. AbilityOne Office of Inspector General
355 E Street, SW, Suite 335
Washington, DC 20024

The Commission has reviewed the results of the OIG FY-23 FISMA assessment of the Commission’s 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 to mitigate the recommendations with estimated timelines.

(1) Risk Assessment, Recommendation #1

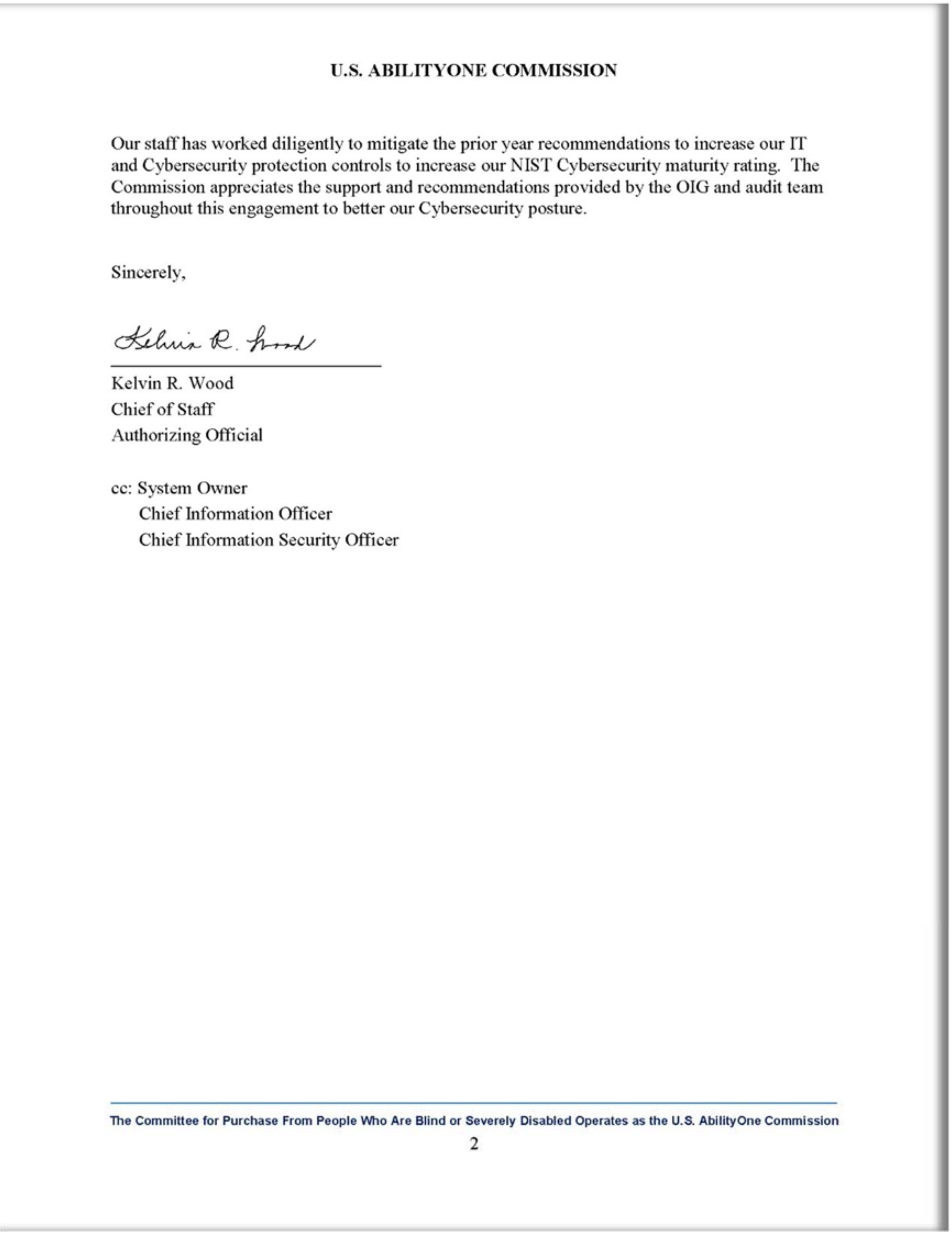
The AbilityOne Commission should implement and undergo an annual Risk Assessment utilizing the latest NIST documents.

The Commission has a performance work statement for an independent risk assessment in FY24. This recommendation is expected to be in compliance by FY24 Q2.

(2) Privacy Policy, Recommendation #2

The AbilityOne Commission has not implemented a privacy policy or program.

The Commission has identified the privacy policy and procedures are not in compliance with NIST-RMF Rev. 5 new guidance. A Privacy Officer has been identified and is in the process of developing the Privacy policy and creating the appropriate procedures to implement the applicable protection controls. This recommendation expected to be in compliance by FY24 Q2.



U.S. ABILITYONE COMMISSION

Our staff has worked diligently to mitigate the prior year recommendations to increase our IT and Cybersecurity protection controls to increase our NIST Cybersecurity maturity rating. The Commission appreciates the support and recommendations provided by the OIG and audit team throughout this engagement to better our Cybersecurity posture.

Sincerely,

Kelvin R. Wood

Kelvin R. Wood
Chief of Staff
Authorizing Official

cc: System Owner
Chief Information Officer
Chief Information Security Officer