U.S. AbilityOne Commission
Office of Inspector General

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

January 30, 2026

MEMORANDUM

TO: Christina Brandt
Interim Chairperson
U.S. AbilityOne Commission

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

FROM: Carla Smith Carla Smith
Acting Inspector General
U.S. AbilityOne Commission OIG

SUBJECT: Fiscal Year 2025 Evaluation of the U.S. AbilityOne Commission's Compliance with the Federal Information Security Modernization Act (FISMA), OIG Report OA-2025-04

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) 2025. The Office of Inspector General engaged the independent public accounting firm Harper, Rains, Knight, & Company, P.A. (HRK) to conduct the annual evaluation and complete the FY 2025 Inspector General (IG) FISMA Reporting Metrics.

The objective of the evaluation was to assess the effectiveness of the Commission's information security program and practices for FY 2025. HRK determined the Commission's maturity levels were consistently implemented and its information security program and practices were effective.

HRK identified one new finding with three corresponding recommendations. The finding was as follows:

1. Unauthorized and unmanaged software was installed and executed

We appreciate the Commission’s assistance during the course of the evaluation. If you have any questions, please contact me or Lauretta A. L. Joseph, Assistant IG for Audit and Evaluation at 571-329-3419 or at ljoseph@oig.abilityone.gov.

cc: Kelvin Wood
Chief of Staff
U.S. AbilityOne Commission

Harper, Rains, Knight & Company

EVALUATION REPORT

ABILITYONE COMMISSION
FEDERAL INFORMATION SECURITY MODERNIZATION ACT
OF 2014 (FISMA)

FOR THE FISCAL YEAR ENDING
SEPTEMBER 30, 2025

Prepared by: Harper, Rains, Knight & Company, P.A.
1425 K ST NW, Suite 1120
Washington, D.C. 20005
202-558-5163
www.hrkcpa.com

Harper, Rains, Knight & Company

TABLE OF CONTENTS

Harper, Rains, Knight & Company

Independent Accountants' Evaluation Report

Interim Chairperson, Committee Members, and Executive Director
U.S. AbilityOne Commission

This report presents the results of our independent evaluation of the U.S. AbilityOne Commission's (the Commission) information security program and practices in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). FISMA requires Federal agencies, including the Commission, to have an annual independent evaluation performed of their information security programs and practices to determine the effectiveness of such programs and practices, and to report the results of the evaluation to the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS). The Commission's Office of Inspector General (OIG) contracted with Harper, Rains, Knight & Company, PA (HRK) to conduct an evaluation of the Commission information security program and practices for Fiscal Year (FY) 2025.

We conducted this evaluation following the Quality Standards for Inspection an Evaluation issued by the Council of the Inspectors General on Integrity and Efficiency (CIGIE). Those standards require that we plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our evaluation objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our evaluation objectives.

The objective of this evaluation was to assess the effectiveness of the Commission's information security program and practices for FY 2025. As part of our evaluation, we responded to the core metrics and supplemental metrics identified in the *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics (IG Metrics) and* the associated *FY 2025 Inspector General FISMA Metrics Evaluator's Guide.* We assessed the maturity levels on behalf of the Commission's OIG to be consistently implemented, which we determined to be effective. We also considered applicable OMB policy and guidelines, National Institute of Standards and Technology's (NIST) standards and guidelines, and the NIST *Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework).*

We determined the Commission has established and maintained a consistently implemented information security program and practices, consistent with applicable FISMA requirements, OMB policy and guidance, DHS guidance, and NIST standards and guidelines. Our evaluation identified the following finding where the Commission's information security program can better protect the confidentiality, integrity, and availability of its information and information systems:

- *Unauthorized and unmanaged software was installed and executed.*

Addressing the open finding will strengthen the Commission’s information security program and practices and contribute to ongoing efforts to maintain reasonable assurance of adequate security over information resources.

This report is for the purpose of concluding on the evaluation objective described above. Accordingly, this report is not suitable for any other purpose. We appreciate the cooperation and courtesies that the Commission personnel extended to us during the execution of this evaluation.

Harper, Rains, Knight & Company, P.A.

January 29, 2026
Washington, D.C.

Background

The Office of the Chief Information Officer (OCIO) is responsible for planning, developing, implementing, and maintaining the Commission's Information Technology (IT) program, policies, standards and procedures. OCIO promotes the application and use of information technologies and administers policies and procedures within the Commission to ensure compliance with related federal laws and regulations, including information security. The Chief Information Officer is the official responsible for carrying out the mission of the OCIO, which is responsible for designing the enterprise information architecture; determining the requirements of the Commission's information systems; and developing the integrated systems for nationwide use. Within the OCIO is the Chief Information Security Officer (CISO) who is the official responsible for carrying out the OCIO responsibilities under FISMA, including IT governance and security, and is the primary liaison to the Commission's authorizing officials, systems owners, and information security officials.

Federal Information Security Modernization Act of 2014[1]

FISMA codifies the Department of Homeland Security's role in administering the implementation of information security policies for federal Executive Branch civilian agencies, overseeing agencies' compliance with those policies, and assisting OMB in developing those policies. The legislation provides DHS authority to develop and oversee the implementation of binding operational directives to other agencies, in coordination and consistent with OMB policies and practices. FISMA also:

- Authorizes DHS to provide operational and technical assistance to other federal Executive Branch civilian agencies at the agency's request;
- Places the federal information security incident center (a function fulfilled by US-CERT) within DHS by law;
- Authorizes DHS technology deployments to other agencies' networks (upon those agencies' request);
- Directs OMB to revise policies regarding notification of individuals affected by federal agency data breaches;
- Requires agencies to report major information security incidents as well as data breaches to Congress as they occur and annually; and
- Simplifies existing FISMA reporting to eliminate inefficient or wasteful reporting while adding new reporting requirements for major information security incidents.

FISMA requires the Commission to develop, document, and implement an agency-wide information security program to protect its information and information systems, including those provided or managed by another agency, contractor, or other source. FISMA also clearly places responsibility on the Commission's OCIO and CISO to develop, implement, and maintain a security program that assesses risk and provides adequate security for the operations and assets of programs and systems under its control.

[1] From overview section of CISA's FISMA page: https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act

Furthermore, OIG must submit to DHS the "Inspector General FISMA Reporting Metrics" that depicts the effectiveness of the agency's information security program.

Fiscal Year 2025 IG Metrics

FISMA requires each agency inspector general (IG), or an independent external evaluator, to conduct an annual independent evaluation to determine the effectiveness of the information security program and practices of its respective agency. OMB, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), and other stakeholders worked collaboratively to develop the FY 2025 IG FISMA Reporting Metrics. The FY 2025 IG FISMA Reporting Metrics represent a continuation of the work started in FY 2022, when the IG metrics reporting process was transitioned to a multi-year cycle.

The multi-year cycle for IG reporting metrics broke out metrics into two categories, core metrics and supplemental metrics. The core metrics represent a combination of Administration priorities, high impact security processes, and essential functions necessary to determine program effectiveness.[2] The supplemental metrics are considered core metrics but represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness. For FY 2025, the supplemental metrics comprise of five new metrics designed to gauge the maturity of agencies' cybersecurity governance practices and implementation of key components of the Zero Trust Architecture (ZTA). These five metrics will be evaluated by IGs and scored in FY 2025. IGs will consider the supplemental metric ratings when making the domain and function level maturity determinations.[3]

The IG FISMA metrics, developed by and in coordination with OMB, CIGIE, and CIO and CISO councils, are aligned with the six function areas in the NIST Cybersecurity Framework 2.0: govern, identify, protect, detect, respond, and recover. The Cybersecurity Framework provides agencies with a common structure for managing and reducing their cybersecurity risks across the enterprise and provides IGs with guidance for assessing the maturity of controls to address those risks.[4]

Objective, Scope, and Methodology

The objective of this evaluation was to assess the effectiveness of the Commission's information security program and practices for the period October 1, 2024, through June 30, 2025. As part of our evaluation, we responded to the core metrics identified in the *FY 2025 Inspector General FISMA Reporting Metrics, the associated FY 2025 Inspector General FISMA Metrics Evaluator's Guide*, and assessed the maturity levels on behalf of the Commission's OIG. We also considered applicable OMB policy and guidelines, National Institute of Standards and Technology's (NIST) standards and guidelines, and the NIST *Cybersecurity Framework*.

[2] From FY 2025 IG FISMA Metrics Evaluator's Guide introduction section, core metrics definition: https://www.cisa.gov/sites/default/files/2025-05/Final%20FY%202025%20IG%20FISMA%20Metrics%20Evaluation%20Guide_05%20May%202025-508.pdf

[3] From FY 2025 IG FISA Metrics Evaluator's Guide introduction section, supplemental metrics definition: Ibid.

[4] Background from the FY 2025 IG FISMA Reporting Metrics, General Instructions section: https://www.cisa.gov/sites/default/files/2025-04/Final%20FY%202025%20IG%20FISMA%20Reporting%20Metrics_Ver%202.0_April%202025-508_0.pdf

To address our evaluation objective, we assessed the overall effectiveness of the Commission's information security program and practices in accordance with Inspector General reporting requirements:

- Cybersecurity Governance (Govern);
- Cybersecurity Supply Chain Risk Management (Govern);
- Risk and Asset Management (Identify);
- Configuration Management (Protect);
- Identity and Access Management (Protect);
- Data Protection and Privacy (Protect);
- Security Training (Protect);
- Information Security Continuous Monitoring (Detect);
- Incident Response (Respond); and
- Contingency Planning (Recover).

We reviewed the Commission's general FISMA compliance efforts in the specific areas defined in DHS' guidance and the corresponding reporting instructions. We considered the internal control structure for the Commission's systems in planning our evaluation procedures. Accordingly, we obtained an understanding of the internal controls over the Commission's systems through interviews and observations, as well as inspection of various documents, including information technology and other related organizational policies and procedures. Our understanding of these systems' internal controls was used to evaluate the degree to which the appropriate internal controls were designed and implemented. When appropriate, we conducted tests using judgmental sampling to determine the extent to which established controls and procedures are functioning as required.

To accomplish our evaluation objective, we:

- Interviewed key personnel and reviewed legal and regulatory requirements stipulated by FISMA;
- Reviewed documentation related to the Commission's information security program, such as security policies and procedures, system security plans, and risk assessments;
- Tested system processes to determine the adequacy and effectiveness of selected controls; and
- Reviewed the status of recommendations in prior year FISMA and related evaluation reports.

The independent evaluation was conducted from April 2, 2025, through July 31, 2025. It covered the period from October 1, 2024, through June 30, 2025.

Criteria

The criteria used in conducting this evaluation included:

- P.L. 113-283, Federal Information Security Modernization Act of 2014;
- FY 2025 Inspector General (IG) Federal Information Security Modernization Act (FISMA) Reporting Metrics;
- FY 2025 IG FISMA Metrics Evaluator's Guide, v 1.0, May 5, 2025;
- NIST SP 800-12, Rev. 1, *An Introduction to Computer Security*: *The NIST Handbook*;

- NIST SP 800-18, Rev. 1, *Guide for Developing Security Plans for Federal Information Systems*;
- NIST SP 800-30, Rev. 1, *Guide for Conducting Risk Assessments*;
- NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*;
- NIST SP 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations: A system Life Cycle Approach for Security and Privacy;*
- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*;
- NIST SP 800-53, Rev. 5, *Security and Privacy Controls for Federal Information Systems and Organizations;*
- NIST *Framework for Improving Critical Infrastructure Cybersecurity* v1.1;
- NIST *Cybersecurity Framework* (CSF) v2.0;
- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*;
- OMB Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*;
- OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*;
- OMB Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*;
- OMB Memorandum M-21-30, *Protecting Critical Software through Enhanced Security Measures*;
- OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*;
- OMB Memorandum M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*;
- OMB Memorandum M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*;
- OMB Memorandum M-22-09, *Moving the U.S. Government to Zero Trust Cybersecurity Principles*;
- OMB Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*;
- OMB Memorandum M-23-16, Update to Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices;*
- OMB Memorandum M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements;*
- Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*;
- DHS CISA Binding Operational Directives (BODs) and Emergency Directives (EDs);
- Federal Cybersecurity Workforce Assessment Act of 2015;
- Federal Identity, Credential, and Access Management Roadmap Implementation Guidance;
- Federal Information Processing Standard (FIPS) Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors; and*
- Other criteria as appropriate.

Results

We evaluated the Commission's information security program and determined it to be effective. We also identified an area that needs improvement. The results of our independent evaluation concluded that the Commission's information security program is generally compliant with the FISMA legislation and is consistent with the functional areas outlined in the NIST Cybersecurity Framework.

Maturity Level Scoring
The maturity level scoring was developed by DHS and OMB. Level 1 (Ad-hoc) is the lowest level and Level 5 (Optimized) is the highest level. The maturity levels are defined as follows:

1. Level 1 (Ad-hoc): Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
2. Level 2 (Defined): Policies, procedures, and strategies are formalized and documented but not consistently implemented.
3. Level 3 (Consistently Implemented): Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
4. Level 4 (Managed and Measurable): Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.
5. Level 5 (Optimized): Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

The summary assessment results for the Commission maturity level assessment by function areas are in ***Exhibit 1***. The five maturity model levels are defined above.

Exhibit 1 – The Commission's Overall Maturity Level Assessment by Function Area for Core Metrics

FISMA NIST Cybersecurity Framework Function Area	FY 2025 Maturity Level (Core & Supplemental Metrics)
Govern[5]	Managed and Measurable (Level 4)
Identify	Managed and Measurable (Level 4)
Protect	Consistently Implemented (Level 3)
Detect	Managed and Measurable (Level 4)
Respond	Consistently Implemented (Level 3)
Recover	Consistently Implemented (Level 3)
Overall Maturity Level	**Consistently Implemented (Level 3)**

The ratings in FY 2025 focused on a calculated average approach, wherein the average of the metrics in a particular domain are used by IGs to determine the effectiveness of individual function areas (govern, identify, protect, detect, respond, and recover) and the overall program.

[5] New function area for FY2025, therefore N/A for FY2024.

Finding and Recommendations

HRK has assessed the effectiveness of the Commission's information system security controls and identified areas in the Commission's information security program that need improvement. The finding and associated recommendations are discussed below.

Finding 1: ***Unauthorized and unmanaged software was installed and executed***

Condition:

HRK observed, with the Commission CISO present during a virtual meeting, an employee download, install, and execute unauthorized software which should have been blocked per the Commission CISO and Commission policy.

Criteria:

NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations, establishes controls for systems and organizations, including the minimum controls required by the provisions of FISMA to protect federal information and information systems.

IG-Metric RAM.03: (*FY 2025 IG FISMA Metrics Evaluation Guide*)
To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting?

> **P-10, Asset Identification**: (*NIST SP 800-37, Rev. 2*)
> Identify assets that require protection.
>
> **CA-7, Continuous Monitoring**: (*NIST SP 800-53, Rev. 5*)
> Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:
>
> a. Establishing system-level metrics to be monitored;
> b. Establishing organization-defined frequencies for monitoring and assessment of control effectiveness;
> c. Ongoing control assessments in accordance with the continuous monitoring strategy;
> d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;
> e. Correlation and analysis of information generated by control assessments and monitoring;
> f. Response actions to address results of the analysis of control assessment and monitoring information; and
> g. Reporting the security and privacy status of the system to applicable personnel or roles on an organization-defined frequency.
>
> **CM-8, System Component Inventory**: (*NIST SP 800-53, Rev. 5*)
>
> a. Develop and document an inventory of system components that:
>   1. Accurately reflects the system;

2. Includes all components within the system;
3. Does not include duplicate accounting of components or components assigned to any other system;
4. Is at the level of granularity deemed necessary for tracking and reporting; and
5. Includes the following information to achieve system component accountability: organization-defined information deemed necessary to achieve effective system component accountability; and

b. Review and update the system component inventory on an organization-defined frequency.

CM-10, Software Usage Restrictions: (*NIST SP 800-53, Rev. 5*)

a. Use software and associated documentation in accordance with contract agreements and copyright laws;
b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

CM-11, User Installed Software: (*NIST SP 800-53, Rev. 5*)

a. Establish organization-defined policies governing the installation of software by users;
b. Enforce software installation policies; and
c. Monitor policy compliance on an organization-defined frequency.

ID.AM-02, Asset Management: (*NIST CSF*)
Inventories of software, services, and systems managed by the organization are maintained.

<u>Cause</u>:

The Commission's software usage restrictions, which restrict applications from being installed through any process other than group policies using Managed Service Identity's (MSI's) in active directory, or through Microsoft Defender and/or Intune, failed to prevent unauthorized installation(s) and execution of software(s).

<u>Effect</u>:

Unauthorized applications may be running in Commission's environment, creating exploitable vulnerabilities.

<u>Recommendation</u>:

Immediate Actions:

1. Review the installed applications on all issued laptops/desktops/endpoints to ensure no unauthorized software is present and take appropriate action if unauthorized software is present.

2. Review the Commission’s "user" setting population to ensure each "user" is properly configured in compliance with Commission's approved Group Policy Objectives (GPO). Make the appropriate corrections to user configurations, as appropriate.
3. Review and update Active Directory settings and Microsoft Defender and Intune policies to ensure unauthorized software cannot be installed.

Long-Term Actions:

1. Schedule regular software evaluations on all issued laptops to ensure compliance with the Commission approved software policy.
2. Ensure that the annual Security Awareness training for all Commission users includes the risks of downloading software.
3. Ensure that the annual Security Awareness training for all network administrators includes the importance of secure configuration management on user devices.

Managements' Response:

Immediate Actions:

1. The Commission is conducting an enterprise-wide review of installed applications on all issued laptops, desktops, and endpoints using CrowdStrike EDR visibility and currently available Microsoft endpoint inventory capabilities. Any unauthorized software identified will be removed, documented, and addressed in accordance with the Commission’s incident response and configuration management procedures.

2. The Commission is reviewing user and device configurations as part of the ongoing migration from hybrid Active Directory to Microsoft Entra ID to ensure users and devices are properly configured in accordance with approved access, identity, and device management requirements. Any misconfigurations identified will be corrected to support least-privilege access and prevent unauthorized software installation.

3. The Commission is reviewing and updating Microsoft Intune configuration and compliance policies to replace legacy GPO-based controls and strengthen enforcement mechanisms that prevent the installation and execution of unauthorized software. In parallel, the Commission is evaluating Microsoft Defender for Endpoint to enhance endpoint security monitoring and control capabilities.

Long-Term Actions:

1. The Commission will establish recurring software inventory and compliance evaluations for all issued endpoints using Intune reporting, CrowdStrike telemetry, and, upon implementation, Microsoft Defender for Endpoint to support continuous monitoring and compliance with approved software policies.

2. Established policy restrictions will prohibit the installation of applications by users.

3. Privileged users have successfully completed role-based training that addresses cybersecurity risks.

Auditors' Response:

The Commission concurred with our recommendations. We believe the Commission’s proposed corrective actions to be responsive to the recommendations. However, Managements’ responses to the auditors’ recommendations, as well as the overall Commission response to this report, found in Appendix A, have not been subject to evaluation procedures and therefore we do not make any conclusion on these responses nor the corrective actions therein. Evaluation procedures will be applied in the next FISMA cycle to these responses and corrective actions.

Informational Observations

HRK has identified additional observations that do not raise to the level of severity for reporting and formal tracking as a finding but should be considered by the Commission in their overall management of its information security program.

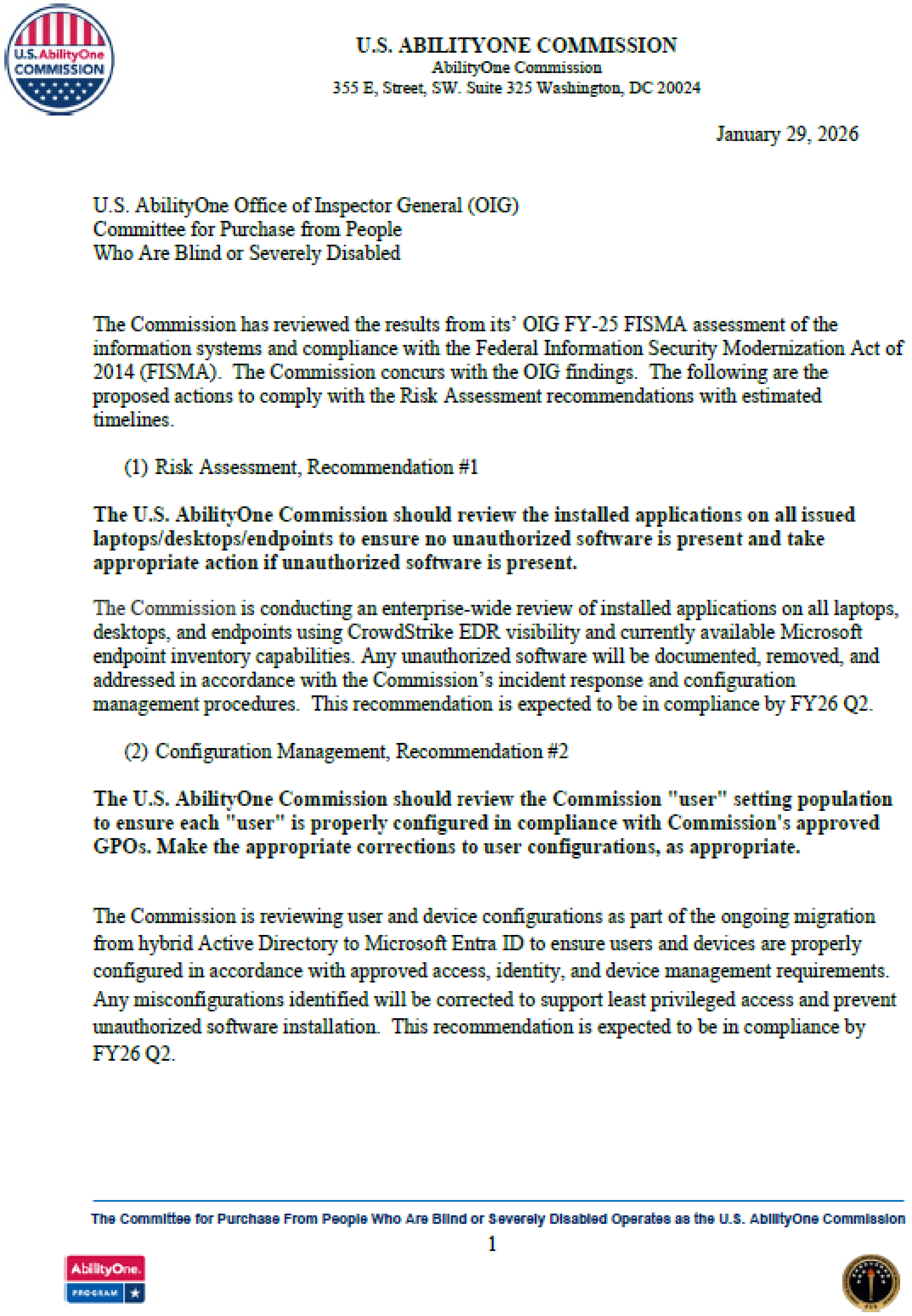
Role Based Security Training

HRK observed that the Commission's OCIO was unable to support the completion of specialized role-based training for one of the five employees sampled. Although this employee took the annual general security training (provided to all Commission staff), the employee either was not assigned, did not complete, or did not maintain the certificate for the specialized role-based training.

If the OCIO employee did not take the specialized security training course, they might not be familiar with some of the more relevant or recent risks or avenues of approach for a malicious actor trying to access the Commission's network and/or data.

The Commission should revisit its required security training standards; revise the security training completion process as necessary to best suit the Commission's needs; and reaffirm those standards to applicable OCIO employees.

Appendix A – Management's Response



U.S. ABILITYONE COMMISSION
AbilityOne Commission
355 E, Street, SW. Suite 325 Washington, DC 20024

January 29, 2026

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

The Commission has reviewed the results from its' OIG FY-25 FISMA assessment of the information systems and compliance with the Federal Information Security Modernization Act of 2014 (FISMA). The Commission concurs with the OIG findings. The following are the proposed actions to comply with the Risk Assessment recommendations with estimated timelines.

(1) Risk Assessment, Recommendation #1

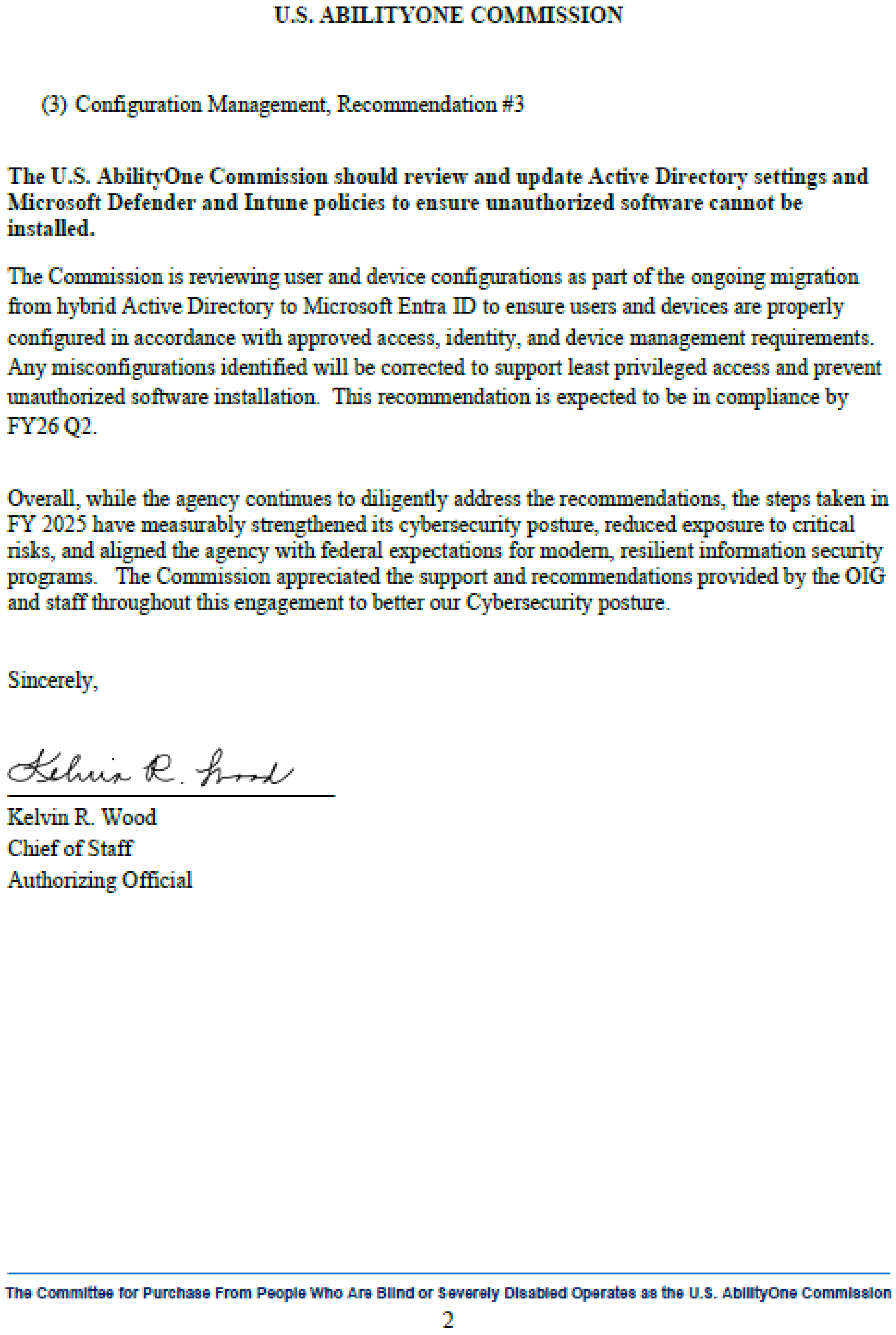
The U.S. AbilityOne Commission should review the installed applications on all issued laptops/desktops/endpoints to ensure no unauthorized software is present and take appropriate action if unauthorized software is present.

The Commission is conducting an enterprise-wide review of installed applications on all laptops, desktops, and endpoints using CrowdStrike EDR visibility and currently available Microsoft endpoint inventory capabilities. Any unauthorized software will be documented, removed, and addressed in accordance with the Commission's incident response and configuration management procedures. This recommendation is expected to be in compliance by FY26 Q2.

(2) Configuration Management, Recommendation #2

The U.S. AbilityOne Commission should review the Commission "user" setting population to ensure each "user" is properly configured in compliance with Commission's approved GPOs. Make the appropriate corrections to user configurations, as appropriate.

The Commission is reviewing user and device configurations as part of the ongoing migration from hybrid Active Directory to Microsoft Entra ID to ensure users and devices are properly configured in accordance with approved access, identity, and device management requirements. Any misconfigurations identified will be corrected to support least privileged access and prevent unauthorized software installation. This recommendation is expected to be in compliance by FY26 Q2.



(3) Configuration Management, Recommendation #3

The U.S. AbilityOne Commission should review and update Active Directory settings and Microsoft Defender and Intune policies to ensure unauthorized software cannot be installed.

The Commission is reviewing user and device configurations as part of the ongoing migration from hybrid Active Directory to Microsoft Entra ID to ensure users and devices are properly configured in accordance with approved access, identity, and device management requirements. Any misconfigurations identified will be corrected to support least privileged access and prevent unauthorized software installation. This recommendation is expected to be in compliance by FY26 Q2.

Overall, while the agency continues to diligently address the recommendations, the steps taken in FY 2025 have measurably strengthened its cybersecurity posture, reduced exposure to critical risks, and aligned the agency with federal expectations for modern, resilient information security programs. The Commission appreciated the support and recommendations provided by the OIG and staff throughout this engagement to better our Cybersecurity posture.

Sincerely,

Kelvin R. Wood

Kelvin R. Wood
Chief of Staff
Authorizing Official