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

355 E Street, SW
Washington, DC 20024-3243

December 9, 2021

MEMORANDUM

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

Kimberly M. Zeich
Executive Director (Acting)
U.S. AbilityOne Commission

FROM: Stefania Pozzi Porter
Inspector General (Acting)
U.S. AbilityOne Commission

Stefania Pozzi Porter

SUBJECT: 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) 2021. 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 2021 IG FISMA Reporting Metrics.

The objective of the evaluation was to assess the effectiveness of the Commission's security program and practices across key functional areas, as of September 30, 2021. The evaluators determined that although the Commission took positive steps to implement policies, procedures and strategies, there are existing improvement opportunities. Specifically, the Commission remediated seven of the nine prior year recommendations leading to their closure at the end of FY 2021. Furthermore, 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. However, the evaluators identified two new findings with two corresponding recommendations. The two findings are as follows:

1. Vulnerabilities are not being remediated in a timely manner, and
2. Configuration settings are not in compliance with Commission policies.

In addition, the evaluators identified 15 open Plan of Actions and Milestones (POA&Ms) related to the control families tested. The evaluators did not perform procedures over these POA&Ms and their remediation, but they are included in the report to ensure continued tracking and resolution by the Commission's IT staff.

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: Irene V. Glaeser
Deputy Executive Director
U.S. AbilityOne Commission

Kelvin R. 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 2021 Evaluation of the U.S. AbilityOne Commission's Compliance with the Federal Information Security Modernization Act

November 24, 2021

McConnell Jones
Diverse Thinking | Unique Perspectives

November 24, 2021

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 2021 (FY21). 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 FY21 Inspector General FISMA Reporting Metrics v1.1, Inspectors General are required to assess the effectiveness of information security programs on a maturity model spectrum. During FY21, there were two findings identified with two corresponding recommendations regarding the Commission's information security program which included:

1. Vulnerabilities not being remediated in a timely manner, and
2. Configuration settings are not in compliance with Commission policies.

Additionally, during FY21, we identified 15 open Plan of Actions and Milestones (POA&Ms) related to the control families being tested. We did not perform procedures over these POA&Ms and their remediation, however we have included a brief overview of them to ensure continued tracking and resolution by the Commission's IT staff.

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. The Commission remediated seven of the nine prior year recommendations, and we deemed them closed as of the end of FY21. We identified two new recommendations during the FY21 evaluation which are detailed within our report. The Commission's comments are included in **Attachment A**.

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

McConnell & Jones LLP

Table of Contents

SECTION **PAGE NUMBER**

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 FY21 IG FISMA Reporting Metrics. The objective of the evaluation was to assess the effectiveness of the Commission's security program and practices across key functional areas as of September 30, 2021.

In accordance with FISMA and Office of Management and Budget (OMB) Memorandum M-21-02, *Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements*, the OIG submitted the IG FISMA Reporting Metrics into the Department of Homeland Security's (DHS) CyberScope application on October 29, 2021. The Commission made progress through implementation of security policies, procedures, and strategies, but lacked quantitative and qualitative measures to assess them.

Under *FY 2021 Inspector General FISMA Reporting Metrics v1.1*, 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 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. The table below summarizes the function and maturity level ratings for FY 2021 FISMA Metrics, as well as the overall rating from the CyberScope system.

FY21 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

The Commission implemented seven of the nine recommendations from the prior year's evaluation. Our evaluation for this year identified that the Commission needs to ensure the implementation of those policies and procedures are assessed over time to manage risks and changing threats. During FY21, there were two findings identified regarding the Commission's information security program which included:

1. Vulnerabilities not being remediated in a timely manner; and
2. Configuration settings are not in compliance with Commission policies

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 FY 2021 findings by control, condition and the number of recommendations.

FY21 FISMA Findings

Control #	Condition	Recommendations
RA-5	Vulnerabilities not being remediated in a timely manner.	1
CM-6 / CM-7	Configuration settings are not in compliance with Commission policies	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 2021 Inspector General FISMA Reporting Metrics v1.1*, 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, Revision (Rev.). 4, *Security and Privacy Controls for Federal Information Systems and Organizations* and 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, 2020 through September 30, 2021 (FY21).

NIST 800-53 Rev. 4 and Rev, 5 have several families and controls within those families[1]. The number of controls vary depending on the security categorization of the respective system (e.g. Low, Moderate, and High), as well as the control enhancements.

For purposes of the FY21 FISMA evaluation, we reviewed 19 control families and 90 associated controls. The scope of our testing included the following new controls, along with testing of the controls from the prior year:

FISMA CONTROLS TESTED DURING FY21	
FAMILY	**CONTROLS**
Access Control (AC)	AC-1, AC-2, AC-5, AC-6, AC-8, AC-11, AC-12, AC-17, AC-19
Awareness and Training (AT)	AT-1, AT-2, AT-3, AT-4
Audit and Accountability (AU)	AU-2, AU-3, AU-6
Security Assessment and Authorization (CA)	CA-1, CA-2, CA-3, CA-5, CA-6, CA-7
Configuration Management (CM)	CM-1, CM-2, CM-3, CM-4, CM-6, CM-7, CM-8, C-9, CM-10
Contingency Planning (CP)	CP-1, CP-2, CP-3, CP-4, CP-6, CP-7, CP-8, CP-9
Identification and Authentication (IA)	IA-1, IA-2, IA-4, IA-5, IA-7, IA-8
Incident Response (IR)	IR-1, IR-4, IR-6, IR-7, IR-8
Media Protection (MP)	MP-3, MP-6
Physical and Environmental (PE)	PE-3
Planning (PL)	PL-4, PL-8
Program Management (PM)	PM-5, PM-7, PM-9, PM-11, PM-30
Personnel Security (PS)	PS-1, PS-2, PS-3, PS-6
Risk Assessment (RA)	RA-1, RA-2, RA-3, RA-5
System and Services Acquisition (SA)	SA-3, SA-4, SA-8, SA-9
System and Communication Protection (SC)	SC-7, SC-8, SC-10, SC-13, SC-18, SC-28

[1] *NIST, Security and Privacy Controls for Federal Information Systems and Organizations, SP 800-53, Revision 4 (April 2013) and NIST, Security and Privacy Controls for Information Systems and Organizations, SP 800-53, Revision 5 (September 2020).*

Privacy Control (AR, SE)	AR-4, AR-5, SE-2
System and Information Integrity (SI)	SI-2, SI-3, SI-4, SI-7
Supply Chain Risk Management (SR)	SR-1, SR-3, SR-5, SR-6, SR-11

Current Year Findings

The results of our FY21 FISMA evaluation identified two findings related to the FISMA controls evaluated, and we provide two associated recommendations as noted below.

01. Vulnerability Management

Condition:

A number of vulnerabilities had not been remediated in a timely manner. The following observations were noted:

- The GSS scans showed 9 devices that had critical, high and medium vulnerabilities.
- The PLIMS scan showed 14 devices with critical, high and medium vulnerabilities.
- The vulnerabilities have had patches released. It was determined that patches with respect to vulnerabilities are not being applied in a timely manner (Critical – ASAP, High – 5 days, Medium – 15 days).

Criteria:

NIST 800-53, Revision 4, Risk Assessment (RA)-5 states:
According to NIST, the organization "remediates legitimate vulnerabilities in accordance with an organizational assessment of risk."

Cause:

Although the Commission IT staff are performing these vulnerability scans in a timely manner, they are not remediating the findings or outcomes of those scans in a timely manner per NIST 800-53, Revision 4.

Risk:

By having vulnerabilities (critical, high and medium) exposed to the Commission, and not remediated in a timely manner, there is the risk that adversaries can take advantage of those weaknesses and gain access to the Commission's data, which ultimately may lead to a lack of integrity and/or confidentiality for the Commission.

Vulnerability scanning includes, for example: (i) scanning for missing and/or out of date patches; (ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and (iii) scanning for improperly configured or incorrectly operating information flow control mechanisms. Remediation is the correction of a vulnerability or eliminating a threat.

Recommendation(s):

1. Scanning should be run on a monthly basis, however if there are medium, high and/or critical vulnerabilities, then they should be remediated, and the scan should be repeated and run again.

Management Response:

The Commission concurred with the finding and recommendations. Management's comments are included in **Attachment A**, which details the Commission's planned actions for completion by December 31, 2021.

Auditor's Response to Management's Comments:

Finding 01, Recommendation 1

The Commission is responsible to ensure that their scanning and vulnerability remediation policies are adequately designed, implemented and being followed as required by the NIST requirements. Evidence of successful and timely remediation of critical, high and medium findings should be maintained to support future evaluations. The OIG and Auditors will review and evaluate the implementation and sustainment of the policy in future evaluations.

02. Configuration Management

Condition:

Obtained and examined the configuration settings depicting the baseline configurations for each of the boundary elements representing the GSS, application, and firewall(s). Based on examination, it was determined that some settings were not in compliance with policy as they had failed checks.

Criteria:

<u>NIST 800-53 Revision 4, CM-6 states:</u>
"The organization:
a. Establishes and documents configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements;
b. Implements the configuration settings;
c. Identifies, documents, and approves any deviations from established configuration settings for [Assignment: organization-defined information system components] based on [Assignment: organization-defined operational requirements]
d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures."

<u>NIST 800-53 Revision 4, CM-7 states:</u>
"The organization:
a. Configures the information system to provide only essential capabilities; and
b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined prohibited or restricted functions, ports, protocols, and/or services]."

Cause:

The Commission IT staff is performing configuration compliance scans periodically, however, the IT staff are not updating the configurations to comply with Commission IT Policy.

Risk:

Failure to properly configure system components to the most restrictive settings compromises the security posture of the system and can lead to unauthorized access, increased vulnerability to attacks, and unauthorized data sharing and data exploitation, all of which compromise the integrity, confidentiality, and availability of the system.

Recommendation(s):

2. Update the configuration settings on the servers to be in compliance with Commission IT Policy and ensure only essential capabilities are being provided.

Management Response:

The Commission concurred with the finding and recommendations. Management's comments are included in **Attachment A**, which details the Commission's planned actions for completion by March 31, 2022.

Auditor's Response to Management's Comments:

Finding 02, Recommendation 2

The Commission is responsible to ensure that systems are configured in compliance with Commission IT policy and that only essential capabilities are running. Evidence of periodic compliance monitoring to ensure configuration settings remain compliant with IT Policy should be maintained to support future evaluations. Furthermore, any deviations from IT Policy should be documented and retained to support any non-compliant configuration settings needed to meet the mission of the organization. The OIG and Auditors will review and evaluate the implementation and sustainment of the policy in future evaluations.

Open POA&Ms

During the FY21 evaluation, we identified 15 open POA&Ms related to the control families being tested. The conditions that generated these POA&Ms were identified by another evaluator during a separate engagement and reported to Commission IT management. We did not perform procedures over these POA&Ms and their remediation, however we have included a brief overview of them below to ensure continued tracking and resolution by the Commission's IT staff.

Open POA&Ms Identified during FY21 FISMA Evaluation		
#	**Control**	**POA&M**
1	**SA-3: System development life cycle**	Obtained the AbilityOne POA&M report and noted two open POA&Ms stating: (1) PLIMS - AbilityOne has no process or deployed tools to perform integrity verification to detect unauthorized changes on the information system (Firmware). (2) AbilityOne GSS - Formal SOP or Guidance not developed for System Development Lifecycle (SDLC) procedures.
2	**SA-4: Acquisition process**	Obtained the AbilityOne POA&M report and noted an open POA&M stating: AbilityOne doesn't require the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.
3	**CA-3: System Interconnections**	Obtained the AbilityOne POA&M report and noted that an Open POA&M exists for this control. It states: MOU,'s or ISA not in place for PLIMS interaction with external systems to AbilityOne.
4	**CP-7: Alternate Processing Site**	Obtained the AbilityOne POA&M for both PLIMS and the GSS which states that an alternate processing site is not implemented.
5	**CP-8: Telecommunications Services**	It was determined through interview and review of artifacts that the environment is maintained within the Azure FedRAMPed environment. Because it is a FedRAMPed environment, it includes the necessary security safeguards. Additionally, because the data resides in the cloud, it is not suseptible to the same security risks. Lastly, due to the nature of the FedRAMPed environment, the data is backed up and telecommunications services are relying on the Azure environment. Noted there was an Open POA&M associated with this control about lack of an alternate telecommunications site.

Open POA&Ms Identified during FY21 FISMA Evaluation		
#	**Control**	**POA&M**
6	**SI-2: Flaw Remediation**	Noted there is an open POA&M associated with this control which states: (1) PLIMS a legacy application that cannot be upgraded to a stable Microsoft baseline, ie. . Microsoft Server 2012 or later. (2) CISA Cyber hygiene scanning revealed 12 total potential vulnerabilities on 5 internet accessible vulnerable hosts. There were 3 distinct open ports, 2 distinct services, and 3 operating systems were detected.
7	**SI-4: Information System Monitoring**	Noted that an Open POA&M exist for this control which states: Remote devices must scan for Malware prior connecting to system network.
8	**SI-7: Software, Firmware and Information Integrity**	Noted that an open POA&M exists for this control which states: Application has no tools to perform integrity verification to detect unauthorized changes on the information system (Firmware)
9	**IA-2: Identification and Authentication (Organizational Users)**	Noted an Open POA&M exists for this control which states: MFA not implemented on the PLIMS voting portal which is public accessible.
10	**IA-2: Identification and Authentication (Organizational Users)**	Noted that an Open POA&M exists for this control: Publicly accessible PLIMS voting portal does not deploy PIV certificate.
11	**IA-8: Identification and Authentication (Non-Organizational Users)**	Noted an Open POA&M exists for this control which states: (1) PIV card and/or MFA not implemented and enforced on systems and devices (2) AbilityOne does not accept and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.
12	**AC-6: Least Privilege**	Noted an Open POA&M exists for this control which states: Admins can see all user data as opposed to being limited to Admin Functions and needing to switch to a non-privileged account for user functions.
13	**AU-2: Audit Events**	Noted there is an Open POA&M that states: SQL events are not audited, monitored, reported, and documented.

Open POA&Ms Identified during FY21 FISMA Evaluation		
#	**Control**	**POA&M**
14	**AU-3: Content of Audit Records**	Noted there is an Open POA&M for this control which states: Audit logs/activity reports are not tracked for PLIMS
15	**SC-7: Boundary Protection**	Noted there is an Open POA&M for this control which states: Update protection controls in PLIMS SSP and logically separate the standard users from the server network

Prior Year Findings

During the FY21 engagement, we reviewed the corrective action status of the findings and recommendations from the FY20 evaluation. The results of our evaluation revealed that the Commission's IT organization made significant progress in addressing the recommendations.

The FY20 IG FISMA evaluation contained 6 findings and 9 associated recommendations. Our evaluation determined that seven recommendations were successfully remediated and deemed closed.

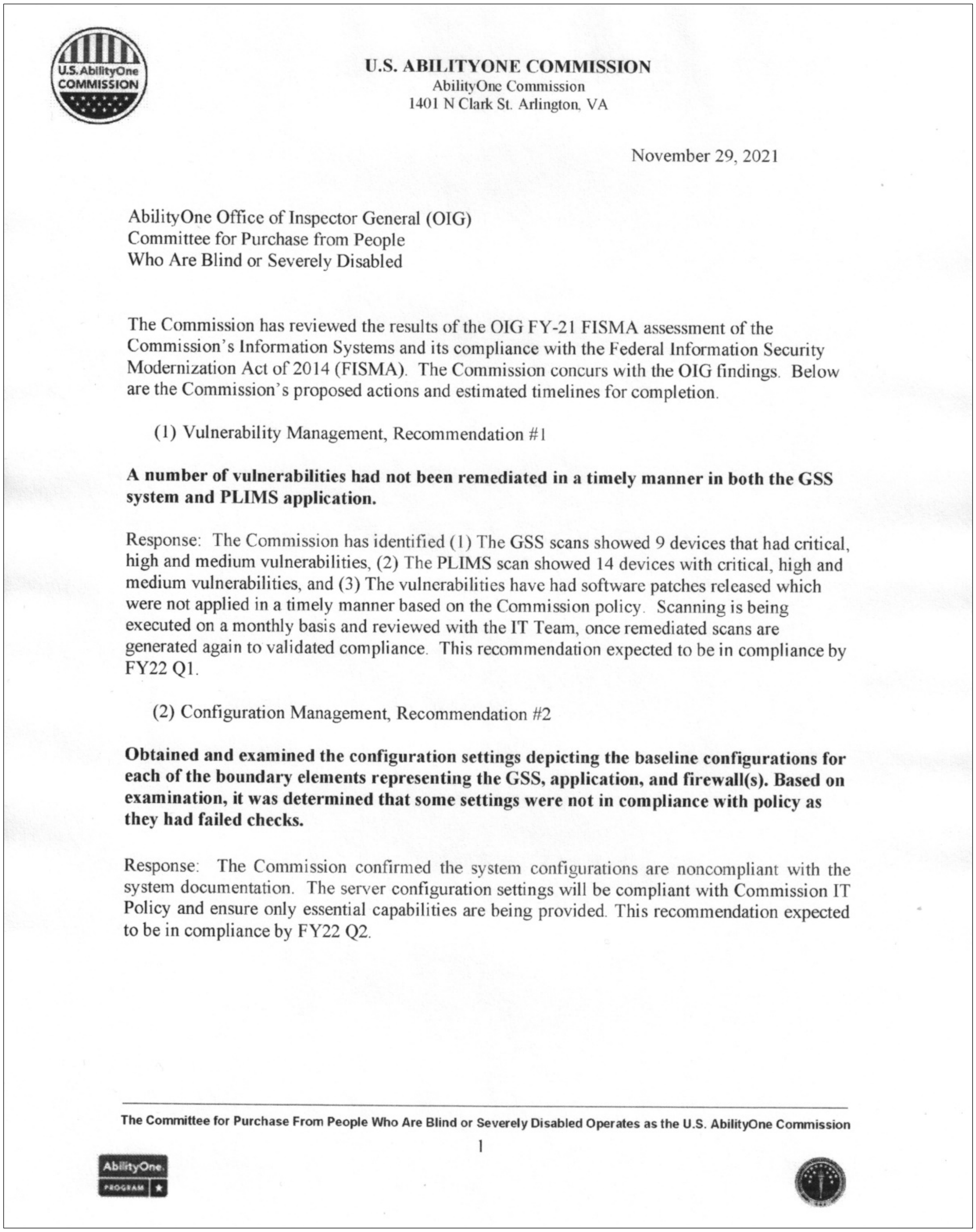
Since FY17, the Commission has deployed additional configuration settings, continued to draft and approve new policies, and deployed scanning to address assessments of controls.

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

STATUS OF FY20 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 an/or high vulnerabilities, then they should be remediated, and the scan should be repeated and run again.	2020-2	Open
Security Assessment and Authorization		
The Commission should identify any deficiencies) through the development of the SSP) and they should be documented on the SAR.	2020-3	Closed
Once the SAR is completed, the Accrediting Official should sign-off on the SAR indicating their acceptance of risk for this system to be in a production environment.	2020-4	Closed
All deficiencies identified on the SAR should then be categorized by risk (low, medium and high) and them formalized POA&Ms should be created. The POA&Ms should contain the hours needed to remediate the deficiency, personnel required, timeline and cost.	2020-5	Closed
Contingency Planning		
Commission IT should ensure that backed up data is encrypted.	2020-6	Closed
Access Controls		
All users should have their IDs automatically disabled after a period of 90 days of inactivity.	2020-7	Closed
Finalize the mobile device policy and ensure that users of the systems adhere to the stipulations outlined within the policy.	2020-8	Closed
Program Management		
Ensure that Commission IT finalizes the Enterprise Architecture policy and then disseminate it to appropriate personnel.	2020-9	Closed

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
AbilityOne Commission
1401 N Clark St. Arlington, VA

November 29, 2021

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

The Commission has reviewed the results of the OIG FY-21 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 and estimated timelines for completion.

(1) Vulnerability Management, Recommendation #1

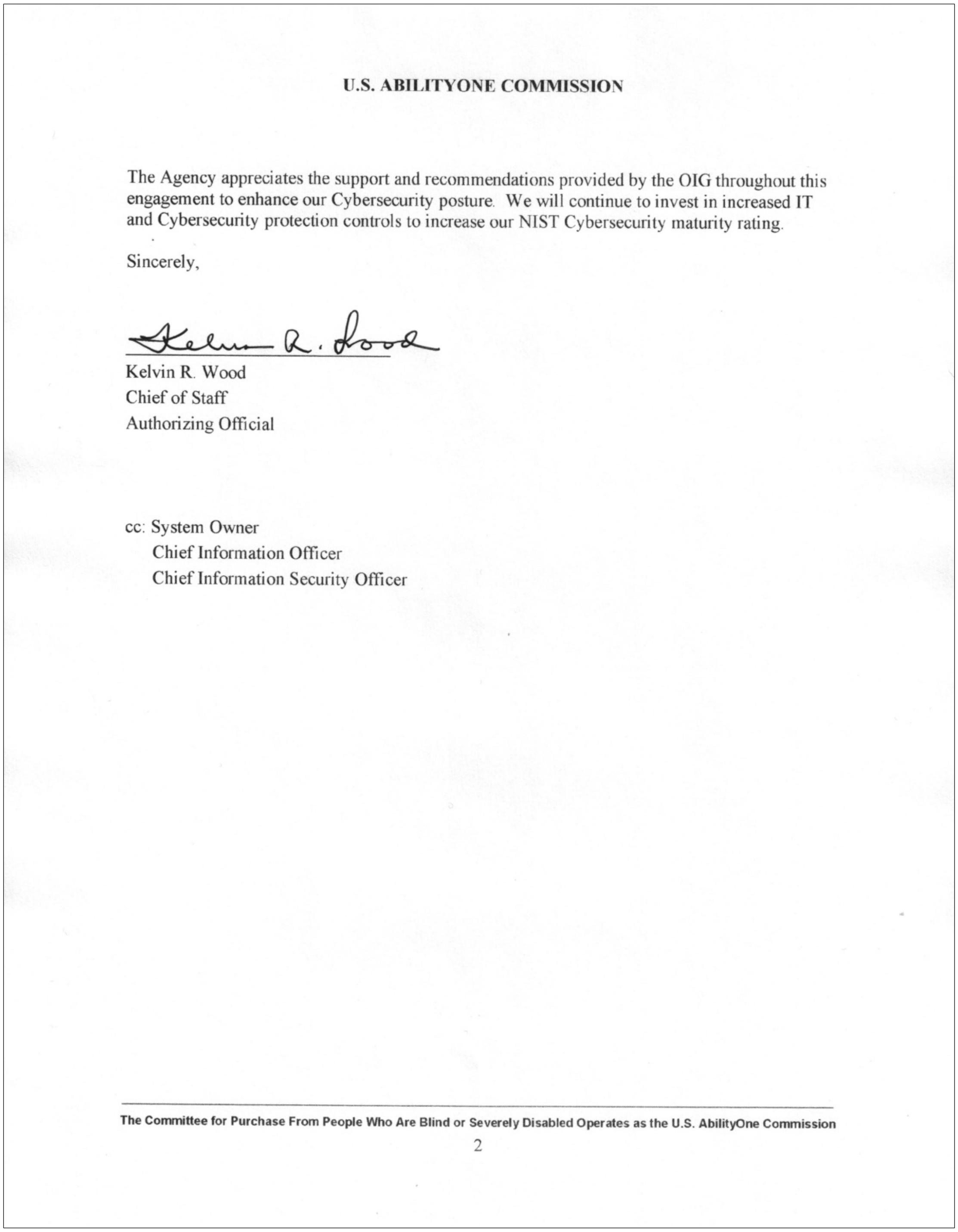
A number of vulnerabilities had not been remediated in a timely manner in both the GSS system and PLIMS application.

Response: The Commission has identified (1) The GSS scans showed 9 devices that had critical, high and medium vulnerabilities, (2) The PLIMS scan showed 14 devices with critical, high and medium vulnerabilities, and (3) The vulnerabilities have had software patches released which were not applied in a timely manner based on the Commission policy. Scanning is being executed on a monthly basis and reviewed with the IT Team, once remediated scans are generated again to validated compliance. This recommendation expected to be in compliance by FY22 Q1.

(2) Configuration Management, Recommendation #2

Obtained and examined the configuration settings depicting the baseline configurations for each of the boundary elements representing the GSS, application, and firewall(s). Based on examination, it was determined that some settings were not in compliance with policy as they had failed checks.

Response: The Commission confirmed the system configurations are noncompliant with the system documentation. The server configuration settings will be compliant with Commission IT Policy and ensure only essential capabilities are being provided. This recommendation expected to be in compliance by FY22 Q2.



U.S. ABILITYONE COMMISSION

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

Kelvin R. Wood
Chief of Staff
Authorizing Official

cc: System Owner
Chief Information Officer
Chief Information Security Officer