Committee for Purchase From People Who Are Blind or Severely Disabled

Office of Inspector General

November 25, 2020

MEMORANDUM

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

FROM: Thomas K. Lehrich
Inspector General

SUBJECT: Evaluation of the U.S. AbilityOne Commission's Compliance with the Federal Information Security Modernization Act, Report No. 21-02

I am pleased to provide, as required by the Federal Information Security Modernization Act of 2014, the results of the annual independent evaluation of the Commission's Information Security Program and Practices for Fiscal Year (FY) 2020. The Office of Inspector General engaged the independent public accounting firm McConnell & Jones LLP (M&J) to conduct the annual evaluation and complete the FY2020 IG FISMA Reporting Metrics. M&J served as the auditor and the Office of the Inspector General (OIG) monitored the contractor's performance.

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, 2020. The Commission made progress through implementation of security policies, procedures, and strategies, but lacked quantitative and qualitative measures to assess them.

During FY20, there were six findings and nine corresponding recommendations regarding the Commission's information security program, including:

1. Vulnerabilities not being remediated in a timely manner

2. Security assessment plan and security assessment report not documented during annual assessment exercises

3. Back-up data not stored with encryption

4. Inactive accounts not automatically disabled after 90 days of inactivity

5. Mobile device usage policy in draft and not finalized, approved or distributed as of year-end

6. Enterprise Architecture Policy is currently in draft and not finalized, approved or disseminated

Under the Inspector General FISMA Reporting Metrics v.1.3, Inspectors Generals (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 the information security program of an agency. The overall assessment of the Commission's FY 2020 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.

M&J determined that the Commission implemented the prior year's three open recommendations. This year, M&J had 6 findings and provided nine new recommendations.

Office of the Inspector General

for

U.S. AbilityOne Commission

FY 2020 Evaluation of the U.S. AbilityOne Commission's Compliance with the Federal Information Security Modernization Act

November 24, 2020

MJ McConnell & Jones LLP
CERTIFIED PUBLIC ACCOUNTANTS
5101 Wisconsin Ave. NW
Suite 210
Washington, D.C. 20016
PH: 202.207.3570
www.mcconnelljones.com

MJ McConnell & Jones LLP
CERTIFIED PUBLIC ACCOUNTANTS

November 24, 2020

Thomas K. Lehrich
Inspector General

We are pleased to provide our report on the information security at the U.S. AbilityOne Commission (Commission) for Fiscal Year (FY) 2020. 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 FY 2019 Inspector General FISMA Reporting Metrics v.1.3, inspectors general are required to assess the effectiveness of information security programs on a maturity model spectrum. During FY20, there were six findings with nine corresponding recommendations regarding the Commission's information security program including:

1. Vulnerabilities not being remediated in a timely manner;
2. Security assessment plan and security assessment report not documented during annual assessment exercises;
3. Back-up data not stored with encryption;
4. Inactive accounts not automatically disabled after 90 days of inactivity;
5. Mobile device usage policy in draft and not finalized, approved or distributed as of year-end; and
6. Enterprise Architecture Policy is currently in draft and not finalized, approved or disseminated

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 2020 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. We closed all prior year recommendations and identified nine new recommendations 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 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 fiscal year (FY) 2020 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, 2020.

In accordance with FISMA and Office of Management and Budget (OMB) Memorandum M-20-02*, Fiscal Year 2019-2020 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 November 2, 2020. The Commission made progress through implementation of security policies, procedures, and strategies, but lacked quantitative and qualitative measures to assess them.

Under *FY 2019 Inspector General FISMA Reporting Metrics v.1.3*, 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 2020 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 FY20 FISMA Metrics, as well as the overall rating from the CyberScope system.

FY20 FISMA Metrics from CyberScope		
Function	**Calculated Maturity Level**	**Assessed Maturity Level**
Function 1: Identify – Risk Management	4 - Managed and Measurable	3 - Consistently Implemented
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 all three 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 FY20, there were six findings regarding the Commission's information security program including:

1. Vulnerabilities not being remediated in a timely manner
2. Security assessment plan and security assessment report not documented during annual assessment exercises
3. Back-up data not stored with encryption
4. Inactive accounts not automatically disabled after 90 days of inactivity
5. Mobile device usage policy in draft and not finalized, approved or distributed as of year-end
6. Enterprise Architecture Policy is currently in draft and not finalized, approved or disseminated

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 FY20 findings by control, condition and the number of recommendations.

FY20 FISMA Findings		
Control #	Condition	Recommendations
RA-5	Vulnerabilities are not being remediated in a timely manner.	2
CA-2, CA-5	Security assessment plan and security assessment report were not documented during annual assessment exercises.	3
CP-9	Back-up data was not stored with encryption.	1
IA-4	Inactive accounts are not automatically disabled after 90 days of inactivity.	1
AC-19	Mobile device usage policy was in draft and not finalized, approved or distributed as of year-end	1
PM-07	Enterprise Architecture Policy is currently in draft and has not been finalized, approved or disseminated.	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 2019 Inspector General FISMA Reporting Metrics v1.3, 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 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, 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, 2019 through September 30, 2020 (FY 2020).

NIST 800-53 Revision 4 has 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 FY 2020 FISMA evaluation, we reviewed 17 control families and 81 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 FY 2020	
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
Maintenance (MA)	MA-1
Media Protection (MP)	MP-3, MP-6
Planning (PL)	PL-2, PL-4, PL-8
Program Management (PM)	PM-5, PM-7, PM-8, PM-9, PM-11
Personnel Security (PS)	PS-1, PS-2, PS-3, PS-6
Risk Assessment (RA)	RA-1, RA-2, 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
System and Information Integrity (SI)	SI-2, SI-3, SI-4, SI-7

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

Current Year Findings

The results of our FY 2020 FISMA evaluation identified six findings related to the FISMA controls evaluated, and we provide nine 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 Firewall scans showed 1 high and 3 medium vulnerabilities. The high vulnerability patch has been available since May 2020 and has not been implemented;
- The Network switch scan showed 1 high and 2 medium on one device; and
- There were 7 high and 2 medium on 2 other devices. The high vulnerabilities have had patches released for several months and have not been implemented.

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 (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. The Commission should follow their vulnerability remediation policies.

2. 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.

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, 2021.

Auditor's Response to Management's Comments:

The Auditors will review and evaluate the remediation actions implemented by the Commission during next year's FISMA evaluation. The third switch referenced in the Commission's response at **Attachment A** increases risk to the organization, and it will require additional attention as there will no longer be vendor support. The Commission needs to ensure that they are taking measures to prevent or detect and correct the potential vulnerabilities that could result from this weakness.

Finding 01, Recommendation 1

The Commission is responsible to ensure that their vulnerability policies are adequately designed, implemented and followed as required by NIST requirements. The OIG and Auditors will review and evaluate the implementation and sustainment of the policy in future evaluations.

Finding 01, Recommendation 2

The Commission is responsible to ensure that their scanning policies are adequately designed, implemented and being followed as required by the NIST requirements. Evidence of the performance of the scanning controls 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. Security Assessment and Authorization

Condition:
A security assessment plan and Security Assessment Report (SAR) are not documented during annual assessment exercises.

Criteria:
NIST 800-53 Revision 4, CA-2 states:
"Assesses the security controls in the information system and its environment of operation to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements."

"Produces a security assessment report that documents the results of the assessment."

NIST 800-53 Revision 4, CA-5 states:
"The organization:
a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system."

Cause:
The Commission IT staff is performing and assessing the controls over the required three year cycles, but they are not identifying the noted deficiencies that result from the assessment within the SAR per NIST 800-53, Revision 4.

Risk:
Without appropriately documenting the implementation status of each of the assessed controls, it will be unlikely that the deficiencies will be remediated in a timely manner. By not tracking POA&Ms, the Commission will not have appropriate funding to remediate deficiencies. Also, vulnerabilities that have not been remediated will remain dormant and expose the Commission to increased risk of exploitation. Without testing all of the controls, and on a continuous basis, there is a high likelihood that exploitation may occur as the controls are not deployed with the latest protective measures.

Recommendation(s):

3. The Commission should identify any deficiencies (through the development of the SSP) and they should be documented on the SAR.
4. Once the SAR is completed, the Accrediting Official (AO) should sign off on the SAR indicating their acceptance of risk for this system to be in a production environment.
5. All deficiencies identified on the SAR should then be categorized by risk (low, medium, and high) and then formalized POA&Ms should be created. The

POA&Ms should contain the hours needed to remediate the deficiency, personnel required, timeline, and cost.

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, 2021.

Auditor's Response to Management's Comments:

Finding 02, Recommendation 3

The Commission is responsible to complete a periodic assessment of the controls and document any deficiencies identified per NIST requirements. There is increased risk to the Commission if the SAR is not complete. Management needs to ensure the completeness of the assessment and the noted deficiencies to ensure successful remediation of all deficiencies. Evidence of the SAR and any related corrective actions should be maintained to support future evaluations. The OIG and Auditors will review and evaluate the SAR in future evaluations.

Finding 02 Recommendation 4

The Commission is responsible to ensure that the SAR is reviewed and approved by the AO, and the approved SAR should be maintained to support future evaluations. The OIG and Auditors will review and evaluate the SAR in future evaluations.

Findings 02, Recommendation 5

The Commission is responsible to develop POA&Ms for all noted deficiencies and report them to the Office of Management and Budget (OMB) per OMB and NIST requirements, including the noted elements cited in our recommendation above. The OIG and Auditors will review and evaluate the POA&Ms in future evaluations.

03. Encryption of Backup Data

Condition:

Backup data is not stored with encryption.

This deficiency has been appropriately remediated, however, it is being reported because it existed as of fiscal year-end.

Criteria:
NIST 800-53 Revision 4, CP-9 states:
"Protects the confidentiality, integrity, and availability of backup information at storage locations."

Cause:
The Commission IT staff did not perform encryption of the data backups per NIST 800-53, Revision 4.

Risk:
Without appropriately maintaining backup data (protection via encryption), the Commission runs the risk that if the primary site has an adverse effect (fire, flood, earthquake, theft, etc.) whereby the data can be accessed without appropriate protective measures, the Commission will likely not be able to restore the data.

Recommendation:

1. IT should ensure that backed up data is encrypted.

Management Response:

The Commission concurred with the finding and recommendations. Management's comments are included in **Attachment A**, which details that the Commission has completed the planned actions as of November 20, 2020.

Auditor's Response to Management's Comments:

Finding 03, Recommendation 6

The Commission implemented corrective actions sufficient to remediate the noted deficiency after September 30th but prior to the date of this report. The OIG and the Auditors will review and evaluate the sustainment of those actions during future evaluations.

04. Access Control

Condition:

Inactive accounts are not automatically disabled after 90 days of inactivity.

Criteria:
NIST 800-53, Revision 4, Identification and Authorization (IA)-4 states:
"e. Disabling the identifier after [Assignment: organization-defined time period of inactivity]."

Cause:
The Commission IT staff disabled the 90-day inactivity setting to alleviate the requirement for senior Commission executives to actively log into the network per NIST 800-53, Revision 4.

Risk:
With users having no automated setting to automatically disable their user ID after a period of inactivity, these users' IDs are open to exploitation because they can be used for gaining access to the network.

Recommendation:

2. All users should have their IDs automatically disabled after a period of 90 days of inactivity.

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, 2020.

Auditor's Response to Management's Comments:

Finding 04, Recommendation 7

The Commission is responsible to ensure that user accounts are disabled as cited above. The Commission is also responsible to ensure this policy is adequately designed, implemented and being followed as required by NIST. Evidence of the termination of these users' access 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.

05. Usage Policy for Mobile Devices

Condition:

A usage policy for mobile devices is currently in draft and has not been finalized, approved or distributed.

This deficiency has been appropriately remediated, however, it is being reported because it existed as of fiscal year-end.

Criteria:
NIST 800-53, Revision 4, Access Control for Mobile Devices (AC-19) states:
"The organization:

a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and
b. Authorizes the connection of mobile devices to organizational information systems."

Cause:
The Commission did not develop a list of acceptable and unacceptable mobile code technologies per NIST 800-53, Revision 4.

Effect:
Without appropriately formalizing the Mobile Device Policy, there is the risk that a user could use an unapproved device or have their approved device without proper security controls, thereby exposing the Commission to exploitation of network data.

Recommendation:

3. Finalize the Mobile Device Policy and ensure that users of the systems adhere to the stipulations outlined within the Policy.

Management Response:

The Commission concurred with the finding and recommendations. Management's comments are included in **Attachment A**, which details that the Commission has completed the planned actions as of November 20, 2020.

Auditor's Response to Management's Comments:

Finding 05, Recommendation 8

The Commission implemented corrective actions sufficient to remediate the noted deficiency after September 30th but prior to the date of this report. The OIG and the Auditors will review and evaluate the sustainment of those actions during future evaluations.

06. Enterprise Architecture Policy

Condition:

An Enterprise Architecture Policy is currently in draft and has not be finalized, approved or disseminated.

Criteria:
NIST 800-53, Revision 4, Enterprise Architecture (PM-07) states:

"The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation."

Cause:
The Commission did not finalize the enterprise architecture policy per NIST 800-53, Revision 4.

Risk:
Without an Enterprise Architecture Policy, there is the risk that the network will not be protected via configuration of appropriate security posture. This can lead to exploitation of the Commission's network data.

Recommendation(s):

4. Ensure that IT finalizes the Enterprise Architecture Policy and then disseminates it to appropriate personnel.

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, 2020.

Auditor's Response to Management's Comments:

Finding 06, Recommendation 9

The Commission is responsible to design and implement the cited policy per NIST requirements. The Commission must complete the final policy, obtain approval and issue the policy. The OIG and Auditors will review and evaluate the policy in future evaluations.

Prior Year Findings

During the FY 2020 engagement, we reviewed the corrective action status of the findings and recommendations from the FY 2019 evaluation. The results of our evaluation revealed that the Commission's IT organization made significant progress in addressing the recommendations.

The FY 2019 IG FISMA evaluation contained 2 findings and 3 associated recommendations.

Since FY 2017, 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 three prior years' open recommendations:

STATUS OF FY 2019 FISMA RECOMMENDATIONS

Status of Recommendations	Year / Rec. #	Status
Continuous Monitoring		
The Commission should identify the critical controls within NIST 800-53. Those critical controls should then be assessed and documented every year.	2019-1	Closed
The Commission should identify the remaining controls in NIST 800-53 (all controls less the critical controls). Those controls should be assessed over a three-year period, where each year 1/3rd of the controls are assessed. They should be assessed throughout the year as opposed to assessing the 1/3rd of the controls at one time.	2019-2	Closed
Encryption		
Ensure that all SQL databases and file servers deploy encryption in accordance with FIPS 140-2.	2019-3	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 20, 2020

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 FY20 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 audit findings and recommendations. Below are the Commission's proposed actions to mitigate the recommendations with estimated timelines.

1. Vulnerability Management. Vulnerabilities are not being remediated in a timely manner. Recommendations included the following:

1. The Commission should follow their vulnerability remediation policies.
2. 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.

Response: The Commission has mediated the vulnerabilities identified in the network firewall and for two of three switches. The third switch is at the End of Life (EOL) stage with no further support from the vendor, so this device will be removed from the network. Rescanned artifacts reflecting mitigation have been provided to the auditor. These recommendations are expected to be implemented and in compliance no later than March 31, 2021.

2. Security Assessment and Authorization. Security assessment plan and security assessment report were not documented during annual assessment exercises. Recommendations included the following:

3. The Commission should identify any deficiencies (through the development of the SSP) and they should be documented on the SAR.
4. Once the SAR is completed, the Accrediting Official (AO) should sign off on the SAR indicating their acceptance of risk for this system to be in a production environment.
5. All deficiencies identified on the SAR should then be categorized by risk (low, medium, and high) and then formalized POA&Ms should be created. The POA&Ms should contain the hours needed to remediate the deficiency, personnel required, timeline, and cost.

The Committee for Purchase From People Who Are Blind or Severely Disabled Operates as the U.S. AbilityOne Commission
1

Response: The Commission will contract for an independent system assessment in FY21 and the results will be documented in the SAR and documented in the system POA&M as applicable. These recommendations are expected to be implemented and in compliance no later than March 31, 2021.

3. Encryption of Backup Data. Back-up data was not stored with encryption. Recommendation follows:

6. IT should ensure that backed up data is encrypted.

Response: The Commission mitigated this discrepancy during the OIG assessment. The audit artifact was provided to the auditors.

4. Access Control. Inactive accounts are not automatically disabled after 90 days of inactivity. Recommendation follows:

7. All users should have their IDs automatically disabled after a period of 90 days of inactivity.

Response: The Commission is currently developing its Architecture Policy for Commission review and implementation. This recommendation is expected to be implemented and in compliance no later than December 31, 2020.

5. Usage Policy for Mobile Devices. Mobile device usage policy was in draft and not finalized, approved or distributed as of year-end. Recommendation follows:

8. Finalize the Mobile Device Policy and ensure that users of the systems adhere to the stipulations outlined within the Policy.

Response: The Commission has updated the Mobile Device Policy to reflect the recommended areas of concern during the OIG assessment. The final policy was provided to the auditors.

6. Enterprise Architecture Policy. Enterprise Architecture Policy is currently in draft and has not be finalized, approved or disseminated. Recommendation follows:

9. Ensure that IT finalizes the Enterprise Architecture Policy and then disseminates it to appropriate personnel.

U.S. ABILITYONE COMMISSION

Response: The Commission is currently developing its Architecture Policy for Commission review and implementation. This recommendation expected to be implemented and in compliance no later than December 31, 2020.

We are confident that the audit team observed that our staff has continued to harden our security countermeasures as we strive 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 WOOD

Digitally signed by KELVIN WOOD
Date: 2020.11.20 14:40:05 -05'00'

Kelvin R. Wood
Chief of Staff
Designated Authorizing Official

cc: System Owner
Chief Information Officer
Information Security Officer