Office of Inspector General

PHONE: 703-603-2124

2331 Mill Road, Suite 505
Alexandria, Virginia 22314-4608

December 19, 2018

MEMORANDUM

FOR: Thomas D. Robinson
Chairperson
U.S. AbilityOne Commission

Tina Ballard
Executive Director

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. 19-02

We are pleased to issue the Office of Inspector General (OIG) report on the information security program of the U.S. AbilityOne Commission (Commission) for fiscal year (FY) 2018. The overall assessment of the Commission's information security program was deemed effective because of the ratings throughout the IG Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics domain. Due to the success demonstrated by the Commission's compliance with FISMA, there are no new recommendations in this report. We found the Commission made significant progress to develop, document, and implement agency-wide information security measures that support its operations. The Commission improved IT security and completed most actions needed from prior year recommendations.

McConnell & Jones LLP, an independent public accounting (IPA) firm, served as the auditor and performed an evaluation on the information security program pursuant to the requirements under FISMA. On December 6, 2018, we provided the draft report to the Commission, and agency comments were received on December 19, 2018. The Agency comments are included in the appendix of the report.

In accordance with FY 2018 IG FISMA Reporting Metrics, the objective of the evaluation was to determine the effectiveness of the information security program and practices of the Commission. The scope of this evaluation focused on the Commission's General Support System (GSS) and related information security policies, procedures, standards, and guidelines.

The FY 2017 IG FISMA evaluation contained 11 findings and 29 associated recommendations. During the FY 2018 evaluation, 25 of the 29 recommendations were implemented and are now closed. Four recommendations from the FY 2017 IG FISMA evaluation remain open for continued remediation in the following areas: vulnerability scanning, system security plan, backups, and configuration changes.

The OIG would like to thank the Commission staff, and especially the Office of Information Technology, for their assistance and cooperation. If you have any questions or need additional information, please contact me.

Enclosure: *Evaluation Report of the U.S. AbilityOne Commission's Compliance with the Federal Information Security Modernization Act of 2014 (FISMA)*

cc: Kimberly M. Zeich, Deputy Executive Director
Kelvin Wood, Chief of Staff
Edward Yang, Chief Information Officer

Executive Summary, Report No. 19-02, December 19, 2018 Evaluation of the U.S. AbilityOne Commission's Compliance with the Federal Information Security Modernization Act (FISMA)

Findings

The overall assessment of the U.S. AbilityOne Commission (Commission) information security program was deemed effective because of the ratings throughout the IG FISMA Reporting Metrics domain. The Commission made significant progress to develop, document, and implement agency-wide information security measures that support its operations. The results of the FY 2018 FISMA evaluation identified that there were no new findings related to the FISMA controls evaluated.

The Commission improved the IT security by addressing 7 of 11 prior findings from the FY 2017 IG FISMA evaluation. Four prior findings are on track for remediation in the areas of: scan vulnerabilities, security assessment and authorization package requirements, contingency training and backups, and configuration changes.

Recommendations

There are no new recommendations to report this year. The Commission implemented 25 of 29 recommendations from FY 2017 IG FISMA evaluation. Four recommendations from the prior year evaluation remain open for continued remediation to enhance the information security policies, procedures and practices.

We will continue to follow the agency's progress.

Objective

In accordance with FY 2018 IG FISMA Reporting Metrics, the objective of the evaluation was to determine the effectiveness of the information security program and practices of the Commission.

Background

FISMA requires each agency IG to conduct an annual independent evaluation of its agency's information security program, practices, and controls for select systems. In FY 2018, IG FISMA Reporting Metrics were developed in a collaborative effort between the Office of Management and Budget (OMB), the Department of Homeland Security (DHS), and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), to develop an evaluation guide to accompany the IG FISMA Metrics.

Office of the Inspector General

U.S. AbilityOne Commission

FY 2018 Evaluation of the U.S. AbilityOne Commission's Compliance with the Federal Information Security Modernization Act

December 19, 2018

MJ
McConnell & Jones LLP
Certified Public Accountants
4828 Loop Central Drive, Suite 1000
Houston, Texas 77081
PH: 713.968.1600
FAX: 713.968.1601
www.mcconnelljones.com

MJ McCONNELL & JONES LLP
CERTIFIED PUBLIC ACCOUNTANTS

December 19, 2018

Thomas K. Lehrich
Inspector General

We are pleased to provide the attached report on the information security at the U.S. AbilityOne Commission (Commission) for Fiscal Year (FY) 2018. The objective of this independent evaluation was to assess the compliance of the Commission's information security policies, procedures, and agency standards and guidelines with the Federal Information Security Modernization Act (FISMA). The scope of the evaluation focused on the Commission General Support System (GSS) and related information security policies, procedures, standards and guidelines.

The overall assessment of the Commission's information security program was deemed effective because of the ratings throughout the IG FISMA Reporting Metrics domain. We did not provide any current year recommendations in this report due to the success demonstrated with the Commission's compliance with FISMA.

The Commission improved IT security and has completed most actions needed on prior recommendations. Four recommendations from the prior year remain open for continued remediation. 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 IT organization for their assistance in helping us meet the objective of our evaluation.

McConnell + Jones LLP

McConnell & Jones LLP

4828 Loop Central, Suite 1000
Houston, TX 77081
PH: 713-968-1600
FAX: 713-968-1601

www.mcconnelljones.com

TABLE OF CONTENTS

SECTION **PAGE NUMBER**

BACKGROUND

On December 17, 2002, the E-Government Act of 2002 (Public Law 107-347) was enacted. Title III of the E-Government Act of 2002, commonly referred to as FISMA, focuses on improving oversight of federal information security programs and facilitating progress in correcting agency information security weaknesses. 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 agency. 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 the Office of Management and Budget (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 agency IG or an independent external auditor as determined by the IG.

McConnell & Jones, on behalf of the Commission OIG, conducted an independent evaluation of the quality 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 with guidance by the OIG.

SCOPE AND METHODOLOGY

The scope of our testing focused on the Commission's 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, 2017 through September 30, 2018 (FY 2018).

NIST 800-53 Revision 4 has several families and controls within those families. 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[1].

For purposes of this FISMA engagement, the scope of testing included the following new controls, along with testing of the controls from the prior year:

FISMA CONTROLS TESTED DURING FY 2017	
FAMILY	**CONTROLS**
Access Control (AC)	AC-2
Audit and Accountability (AU)	AU-2, AU-4, AU-6
Security Assessment and Authorization (CA)	CA-2, CA-5, CA-6, CA-7
Configuration Management (CM)	CM-3, CM-8
Contingency Planning (CP)	CP-2, CP-3, CP-4, CP-6, CP-9, CP-10, CP-11, CP-12
Identification and Authentication (IA)	IA-4, IA-5
Incident Response (IR)	IR-2, IR-3, IR-4, IR-5, IR-6, IR-8
Physical and Environmental Protection (PE)	PE-2, PE-3, PE-6, PE-8, PE-10, PE-11, PE-13, PE-14, PE-15, PE-18, PE-19, PE-20
Planning (PL)	PL-2, PL-4
Personnel Security (PS)	PS-4, PS-5
Risk Assessment (RA)	RA-5

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

FISMA CONTROLS TESTED DURING FY 2018	
FAMILY	**CONTROLS**
Configuration Management	CM-9
Maintenance	MA-2
Media Protection	MP-4, MP-5, and MP-6
Awareness and Training	AT-2 and AT-3
Access Controls	AC-7, AC-8, AC-11, and AC-17

EXECUTIVE SUMMARY

The Commission OIG engaged McConnell & Jones to perform a FISMA evaluation and to assist with preparing Cyberscope metrics, which are reported to OMB. The Cyberscope IG FISMA metrics reflected the status of the Commission's compliance as of September 30, 2018. The OIG reported those metrics directly to OMB. During the performance of the FISMA evaluation, McConnell & Jones noted significant progress. These findings and the associated recommendations are intended for the sole and express use of the Commission OIG and Commission management.

The Commission has made great strides with respect to implementing 25 of 29 recommendations from the prior year. Our evaluation identified that the Commission needs to continue developing policies and procedures and ensure the implementation of those policies and procedures in a timely manner. We identified areas for further improvements including, but not limited to, vulnerability scanning, System Security Plan (SSP), adopting cloud services from authorized vendor(s) that meet agency requirements, configuration management and change processes.

The overall assessment of the Commission's information security program was deemed effective because of the ratings throughout the IG FISMA Reporting Metrics domain. The domain ratings are scored through the CyberScope platform and the Level 4, Managed and Measurable, reached by the Commission represents the effective level of security. One of the goals of the maturity model reporting approach is to ensure consistency in IG FISMA evaluations across the Federal government. In FY 2018, a collaborative effort amongst OMB, the Department of Homeland Security (DHS), and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) developed an evaluation guide to accompany the IG FISMA metrics. We used the guidance as part of the FISMA evaluation criteria.

FINDINGS

The results of our FY 2018 FISMA evaluation identified there were no new findings related to the FISMA controls evaluated.

The FY 2017 IG FISMA evaluation contained 11 findings and 29 associated recommendations. During FY 2018, we noted that 25 of the 29 recommendations were implemented and have been closed based on analysis performed to assess implemented actions in given areas.

The Commission made significant strides in closing the FY 2017 recommendations. They deployed configuration settings, drafted and approved policies, installed equipment in the server room, and deployed various logs and reviews. The Commission hired an independent contractor to implement improvements and ensure effective remediation was accomplished. Additionally, Commission IT staff were proactive in anticipating the new controls selected for FY 2018 demonstrating continued improvement.

Management's response:

Please refer to the Commission's response, included as **Attachment A**, which details management's completion of planned actions.

Auditor's comment to management's response:

The auditor acknowledges management's efforts to address the four remaining recommendations from FY 2017 FISMA evaluation and the milestones anticipated appear appropriate. These recommendations related to the following prior year findings:

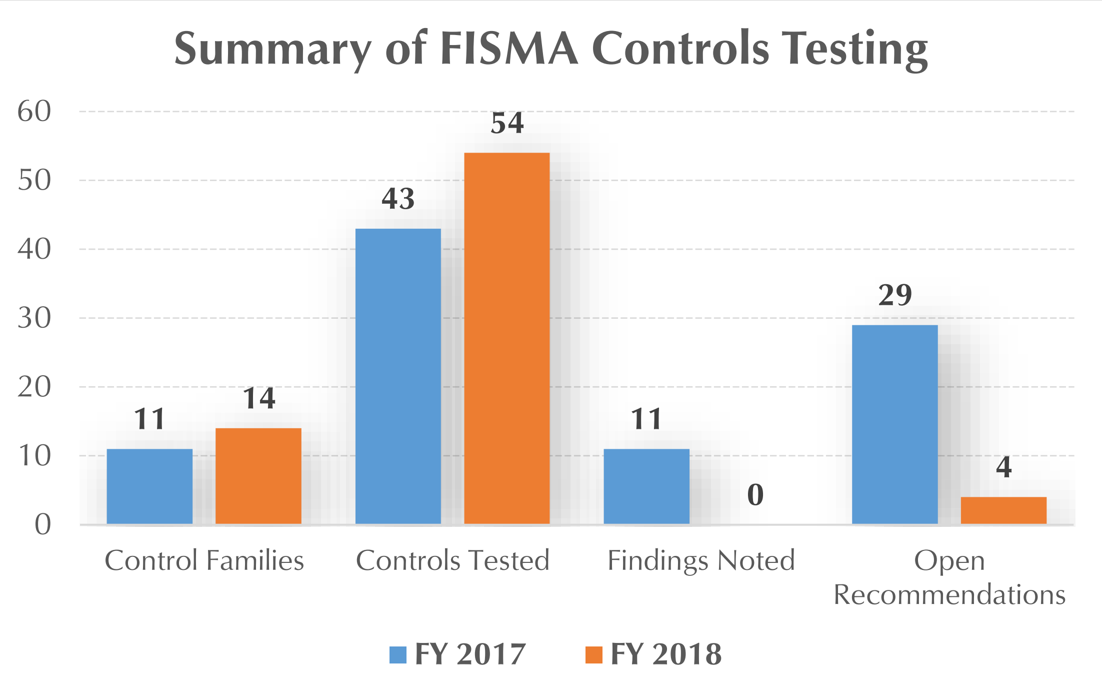
- Timely remediation of vulnerabilities
- SA&A package requirements
- Contingency training and backups
- Configuration changes

The proposed corrective actions meet the intent to address and remediate the noted findings and recommendations. The OIG plans to follow up on the Commission's implemented actions to ensure the recommendations are fully addressed.

PRIOR YEAR FINDINGS

During the FY 2018 engagement, we reviewed the corrective action status of the findings and recommendations from the FY 2017 evaluation. The results of our evaluation revealed that the Commission's IT organization made significant progress in addressing the noted recommendations. Twenty-five (25) recommendations were successfully remediated, verified and deemed closed.

The graph below depicts a comparative analysis of the FY 2017 and FY 2018 FISMA testing of controls.



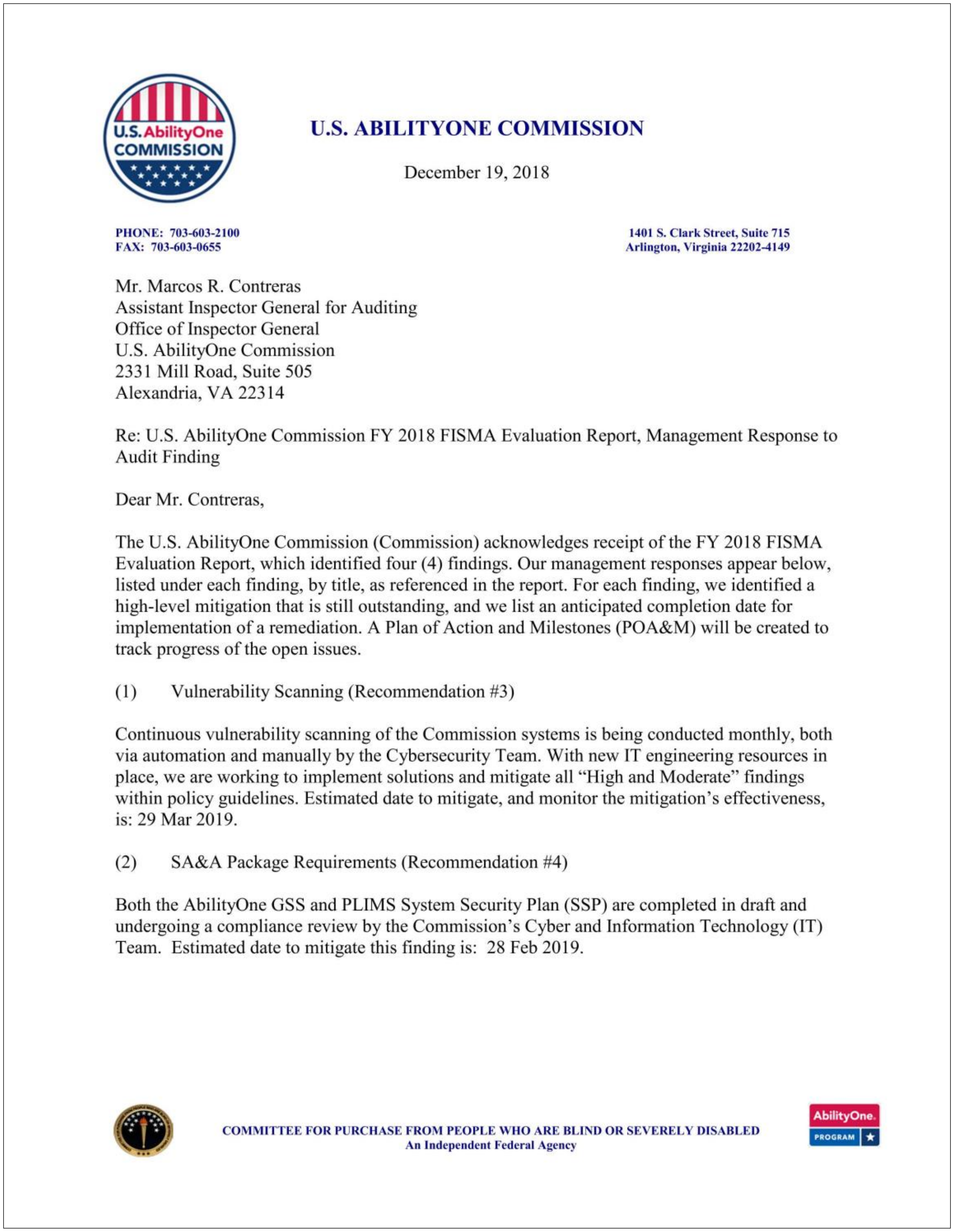
The table below details the recommendations which have been closed during FY 2018, as well as the four (4) open recommendations which require further remediation.

FY 2017 FISMA RECOMMENDATIONS		
Status of Recommendations	**Year / Rec. #**	**Status**
Timely Remediation of Vulnerabilities		
The Office of Information Technology (OIT) established a formalized policy for how the review, documentation, and remediation of vulnerabilities in terms of risk classification should be captured in a timely manner (high, medium, and low). Industry best practices dictate remediation of high vulnerabilities within one business day and medium vulnerabilities within three to five (5) business days.	2017 – 1	Closed
The Commission implemented procedures to ensure vulnerability remediation policies are operating.	2017 – 2	Closed
Vulnerability 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 run again.	2017 – 3	Open
SA&A Package Requirements		
An SSP should be developed, then reviewed and approved by the Chief Information Officer (CIO), whereby all controls within NIST 800-53 are documented as to their implementation status.	2017 – 4	Open
An ISCP was developed, reviewed and approved by the CIO, whereby all critical elements (hardware and software) are addressed in terms of their reconstitution of data.	2017 – 5	Closed
The RoB was updated and signed by employees as evidence of adherence to RoB stipulations, which includes the latest NIST 800-53 requirements such as social media and networking restrictions.	2017 – 6	Closed
The Commission identified deficiencies (through the development of the SSP) and documented the Security Assessment Report (SAR).	2017 – 7	Closed
The SAR was completed, the Accrediting Official (AO) signed off on the SAR indicating their acceptance of risk for this system to be in a production environment.	2017 – 8	Closed
All deficiencies identified on the SAR were categorized by risk (low, medium, and high) and then formalized POA&Ms were created. The POA&Ms contained the hours needed to remediate the deficiency, personnel required, timeline, and cost.	2017 – 9	Closed

FY 2017 FISMA RECOMMENDATIONS		
Status of Recommendations	**Year / Rec. #**	**Status**
Personnel Termination/Transfer		
The OIT established a formal policy and implemented procedures for timely separation, removal and/or updates to users' access. Industry best practices are to remove separated users within five (5) business days and updated transferred users within five (5) business days.	2017 – 10	Closed
Physical and Environmental Controls		
The Commission implemented controls to ensure that only those with appropriate authorizations are permitted into the server room (e.g. the use of electronic badges, sign-in sheet, and controlled entry access).	2017 – 11	Closed
Video monitoring has been implemented and is continuous without interruption inside the server room. Video is maintained for at least one month before being overwritten.	2017 – 12	Closed
Worked with property management to enhance the IT server room by: installing a fire extinguisher, adjusting humidity levels to ensure humidity is not below 30% or above 50%, identifying and checking the water line to ensure the line is working as intended, and installing and testing emergency lighting annually.	2017 – 13	Closed
Contingency Training and Backups		
IT should store incremental and full backups offsite. If backups are to be stored with a third-party provider, then this vendor must be FedRamp certified.	2017 – 14	Open
All IT personnel (both employees and contractors) received annual contingency training.	2017 – 15	Closed
ISCP was finalized and is being tested annually to ensure that IT personnel are prepared for a disaster and back-ups are operational.	2017 – 16	Closed
Configuration Changes		
Established and implemented a process to document all changes, with formalized approvals prior to the change, and capture evidence of the testing results.	2017 – 17	Closed
Segregation of duties have been implemented between environments so that those making the changes are different from those personnel that approve the changes.	2017 – 18	Closed
Each year, a sample of changes should be reviewed to ensure they comply with Commission procedures.	2017 – 19	Open

FY 2017 FISMA RECOMMENDATIONS		
Status of Recommendations	**Year / Rec. #**	**Status**
Incident Response Training and Testing		
Implemented Incident Response Plan and annual testing, review the results and make updates as necessary.	2017 – 20	Closed
All IT personnel (both employees and contractors) were provided with incident response training which will continue annually.	2017 – 21	Closed
Access Authorization Management		
Controls have been implemented to ensure all users' access rights upon initiation have been reviewed, approved, and maintained for subsequent investigations and/or incident response.	2017 – 22	Closed
Annual employee access reviews have been instituted to ensure permissions remain commensurate with their job functions.	2017 – 23	Closed
Annual reviews of admin users' account authorizations have been implemented to ensure that permissions remain appropriate.	2017 – 24	Closed
Complexity Settings		
Controls have been implemented to ensure that all users have their IDs automatically disabled after a period of 120 days of inactivity.	2017 – 25	Closed
Audit Events, Reviews and Updates		
Audit settings have been updated so that "Privileged Use", "Policy Change", and "Account Management" are set to both success and failure.	2017 – 26	Closed
Audit logs are being reviewed by both IT and management personnel within the Commission on a monthly basis and investigation or corrective actions are being taken accordingly.	2017 – 27	Closed
Continuous Monitoring		
The Commission has identified the critical controls within NIST 800-53. Those critical controls are being annually assessed and documented.	2017 – 28	Closed
The Commission has identified the remaining controls in NIST 800-53 (non-critical controls) which should be assessed over a three-year period. Each year, 1/3rd of the controls are continuously being assessed throughout the year, as opposed to assessing 1/3rd of the controls at one time.	2017 – 29	Closed

ATTACHMENT A: COMMISSION'S COMMENTS



U.S. ABILITYONE COMMISSION

December 19, 2018

PHONE: 703-603-2100
FAX: 703-603-0655

1401 S. Clark Street, Suite 715
Arlington, Virginia 22202-4149

Mr. Marcos R. Contreras
Assistant Inspector General for Auditing
Office of Inspector General
U.S. AbilityOne Commission
2331 Mill Road, Suite 505
Alexandria, VA 22314

Re: U.S. AbilityOne Commission FY 2018 FISMA Evaluation Report, Management Response to Audit Finding

Dear Mr. Contreras,

The U.S. AbilityOne Commission (Commission) acknowledges receipt of the FY 2018 FISMA Evaluation Report, which identified four (4) findings. Our management responses appear below, listed under each finding, by title, as referenced in the report. For each finding, we identified a high-level mitigation that is still outstanding, and we list an anticipated completion date for implementation of a remediation. A Plan of Action and Milestones (POA&M) will be created to track progress of the open issues.

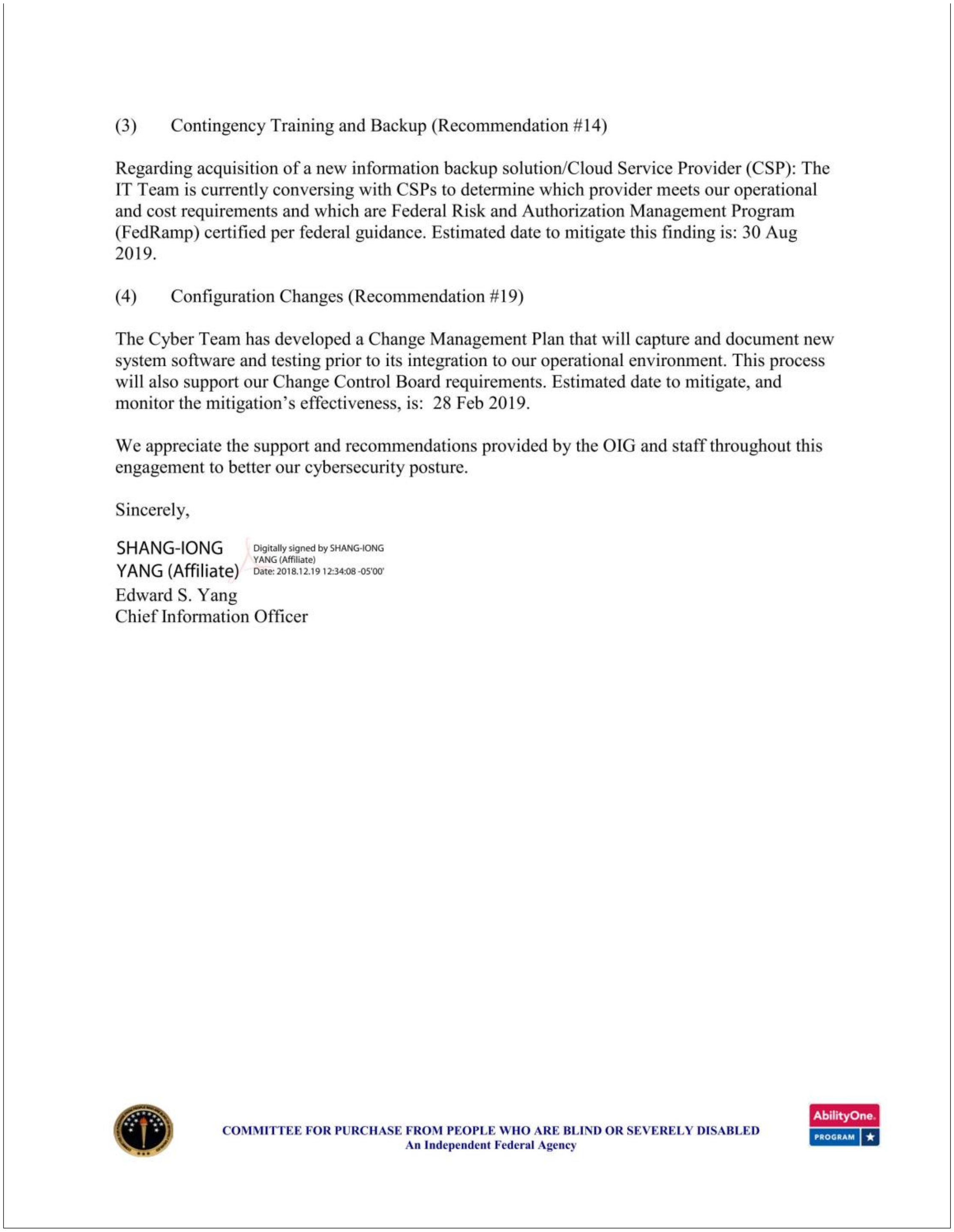
(1) Vulnerability Scanning (Recommendation #3)

Continuous vulnerability scanning of the Commission systems is being conducted monthly, both via automation and manually by the Cybersecurity Team. With new IT engineering resources in place, we are working to implement solutions and mitigate all "High and Moderate" findings within policy guidelines. Estimated date to mitigate, and monitor the mitigation's effectiveness, is: 29 Mar 2019.

(2) SA&A Package Requirements (Recommendation #4)

Both the AbilityOne GSS and PLIMS System Security Plan (SSP) are completed in draft and undergoing a compliance review by the Commission's Cyber and Information Technology (IT) Team. Estimated date to mitigate this finding is: 28 Feb 2019.

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



(3) Contingency Training and Backup (Recommendation #14)

Regarding acquisition of a new information backup solution/Cloud Service Provider (CSP): The IT Team is currently conversing with CSPs to determine which provider meets our operational and cost requirements and which are Federal Risk and Authorization Management Program (FedRamp) certified per federal guidance. Estimated date to mitigate this finding is: 30 Aug 2019.

(4) Configuration Changes (Recommendation #19)

The Cyber Team has developed a Change Management Plan that will capture and document new system software and testing prior to its integration to our operational environment. This process will also support our Change Control Board requirements. Estimated date to mitigate, and monitor the mitigation's effectiveness, is: 28 Feb 2019.

We appreciate the support and recommendations provided by the OIG and staff throughout this engagement to better our cybersecurity posture.

Sincerely,

SHANG-IONG
YANG (Affiliate)

Digitally signed by SHANG-IONG
YANG (Affiliate)
Date: 2018.12.19 12:34:08 -05'00'

Edward S. Yang
Chief Information Officer

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