Office of Inspector General

PHONE: 703-603-2124

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

December 8, 2017

MEMORANDUM

FOR: James M. Kesteloot
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. 18-01

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) 2017. Agency management comments are included to the appendix of the report.

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 the Federal Information Security Modernization Act of 2014 (FISMA). On November 17, 2017, we provided the draft report to the Commission, and agency comments were received on November 30, 2017 in a timely manner.

In accordance with FY 2017 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.

We found the Commission continues to make positive efforts to develop, document, and implement agency-wide information security measures that support its operations and assets. The inventory management maintained an accurate inventory of the Commission's information systems and hardware assets.

The findings from the evaluation demonstrate that improvements are needed in the policies and procedures to achieve better results for the agency-wide information security program. The evaluation measured the effectiveness of the information security programs on a maturity model spectrum, and found the Commission information security program did not meet the FY 2017 IG FISMA Reporting metrics definition of effective.[1]

The FY 2017 IG FISMA Reporting Metrics represent a continuation of work that begun in FY 2016, when the IG metrics were aligned with the five function areas in the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework). The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise and provides OIGs with guidance for assessing the maturity of controls in several areas.

The report contains 29 recommendations to improve the overall security program to meet the IG FISMA Reporting metrics. The recommendations address areas including: scanning vulnerabilities, security assessment and authorization documentation, user access for terminated/transferred personnel, physical and environment controls, contingency training and backups, configuration changes, incident response training and testing, access authorization management, complexity settings, audit events, reviews and updates, and continuous monitoring. We will continue to follow the Commission's actions to address the intent of the recommendations and report the status of those actions in our semiannual reports to Congress.

The OIG would like to thank Commission staff, and especially the Office of Information Technology (OIT), for their assistance and cooperation. If you have any questions or need additional information, please contact me or Marcos R. Contreras, Assistant Inspector General for Auditing.

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

cc: Michael Rogers, Chief of Staff
Barry Lineback, Acting Deputy Executive Director
Edward Yang, Chief Information Officer

---

[1] Security control *effectiveness* addresses the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment or enforcing/mediating established security policies. *NIST Special Publication 800-53, Rev. 4, Security and Privacy of Controls for Federal Information Systems and Organizations* (April 2013, includes updates as of 01-22-2015), page 1, footnote 5.

Office of Inspector General

Executive Summary, Report No. 18-01, December 8, 2017

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

Findings

The U.S. AbilityOne Commission continues to make positive efforts to develop, document, and implement agency-wide information security measures that support its operations and assets. The inventory management maintained an accurate inventory of the Commission's information systems and hardware assets.

The findings from the evaluation demonstrate that improvements are needed in the policies and procedures to achieve better results for the agency-wide information security program. The findings address 11 areas including: scanning vulnerabilities, security assessment and authorization documentation, user access for terminated/transferred personnel, physical and environment controls, contingency training and backups, configuration changes, incident response training and testing, access authorization management, complexity settings, audit events, reviews and updates, and continuous monitoring. The evaluation measured the effectiveness of the information security program on a maturity model spectrum, and found the Commission information security program did not meet the FY 2017 IG FISMA Reporting metrics definition of effective.

Recommendations

The report contains 29 recommendations to improve the security program to meet the IG FISMA Reporting metrics. When implemented, the recommended actions should strengthen the IT system and assist the Commission in becoming FISMA compliant. In the management response, the Commission comments outlines actions that are underway or will be taken to strengthen the Commission's information security program.

We will continue to follow the agency's progress in addressing these recommendations as part of future oversight work.

Objective

In accordance with FY 2017 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 2017 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), in consultation with the Federal Chief Information Officer (CIO) Council. The Framework helps promote consistent and comparable metrics and criteria in the CIO and IG metrics processes while providing agencies with a meaningful assessment of the effectiveness of their information security program.

OFFICE OF THE INSPECTOR GENERAL

U.S. ABILITYONE COMMISSION

FY 2017 Evaluation of the U.S. AbilityOne Commission's Compliance with the Federal Information Security Modernization Act

December 8, 2017

MJ McCONNELL & JONES LLP
CERTIFIED PUBLIC ACCOUNTANTS
4828 Loop Central Drive, Suite 1000
Houston, TX 77081
ph: 713.968.1600
fax: 713.968.1601
www.mcconnelljones.com

MJ McConnell & Jones LLP
CERTIFIED PUBLIC ACCOUNTANTS

December 8, 2017

Thomas K. Lehrich
Inspector General

We are pleased to provide the attached final report on the information security at the U.S. AbilityOne Commission (Commission) for Fiscal Year (FY) 2017. McConnell & Jones LLP (McConnell & Jones) leveraged the expertise of our audit and information technology (IT) resources on the engagement team for assistance with this mandated review.

The objectives of this independent evaluation of the Commission information security program included evaluating its security posture by assessing compliance with the Federal Information Security Modernization Act (FISMA), as amended and related information security policies, procedures, standards and guidelines. The scope of the evaluation focused on the Commission General Support System (GSS) and related information security policies, procedures, standards and guidelines.

The Commission continues to develop and make improvements in the agency's IT security. However, weaknesses continue to exist which require remediation. This report contains 29 recommendations that address 11 findings related to controls and control enhancements, and the agency management 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 objectives of our evaluation.

McConnell & Jones LLP

4828 Loop Central, Suite 1000
Houston, TX 77081
Phone: 713.968.1600
Fax: 713.968.1601

WWW.MCCONNELLJONES.COM

MJ

TABLE OF CONTENTS

SECTION **PAGE NUMBER**

BACKGROUND 1

SCOPE AND METHODOLOGY 2

EXECUTIVE SUMMARY 3

CURRENT FINDINGS 3

1. TIMELY REMEDIATION OF VULNERABILITIES 4

2. SA&A PACKAGE REQUIREMENTS 5

3. PERSONNEL TERMINATION / TRANSFER 8

4. PHYSICAL AND ENVIRONMENTAL CONTROLS 9

5. CONTINGENCY TRAINING AND BACKUPS 11

6. CONFIGURATION CHANGES 13

7. INCIDENT RESPONSE TRAINING AND TESTING 15

8. ACCESS AUTHORIZATION MANAGEMENT 16

9. COMPLEXITY SETTINGS 18

10. AUDIT EVENTS, REVIEWS, AND UPDATES 19

11. CONTINUOUS MONITORING 20

ATTACHMENT A – COMMISSION'S RESPONSE 21

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.

FISMA assigns specific responsibilities to agency heads and Inspectors General (IGs). 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 performed on their information security programs and practices and to report the evaluation results to OMB. FISMA states that the independent evaluation is to be performed by the agency IG or an independent external auditor as determined by the IG. Implementing adequate information security controls is essential to ensuring an organization can effectively meet its mission.

McConnell & Jones LLP, on behalf of the Commission OIG, conducted an independent evaluation of the quality and compliance of the Commission's information security program with applicable federal computer security laws and regulations. McConnell & Jones' evaluation focused on the Commission's information security program as required by FISMA, as amended. This report was prepared by McConnell & Jones with guidance by the OIG. In particular, the FY 2017 IG FISMA Reporting Metrics requires the annual independent evaluation to determine the effectiveness of the information security program and practices of the respective agency.

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 our testing through inquiry of Commission personnel, observation of activities, inspection of relevant documentation, and the performance of technical security testing. More specifically, 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. For example, testing covered system security plans, access controls, risk assessments, personnel security, contingency planning, identification / authentication and auditing. Our testing was for the period October 1, 2016 through September 30, 2017 (FY 2017).

NIST 800-53, Rev. 4[1], has several families and controls within those families. The number of controls will 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 this FISMA engagement, the scope of our testing included the following controls:

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).*

EXECUTIVE SUMMARY

The Commission OIG engaged McConnell & Jones to perform a FISMA evaluation and to assist with preparing CyberScope metrics, which are reported to the Office of Management and Budget (OMB). The CyberScope metrics reflected the status of the Commission's compliance as of September 30, 2017, and Commission management reported those metrics directly to OMB. During the performance of the FISMA evaluation, McConnell & Jones noted deficiencies and those findings, along with the associated recommendations, are detailed below. These findings and the associated recommendations are intended for the sole and express use of the Commission OIG and Commission management.

Fiscal year (FY) 2017 was the second time that the Commission has undergone a FISMA evaluation. The Commission is a relatively new Federal agency and the Commission's IT infrastructure is continuing to be developed. Although the results of this evaluation revealed a number of deficiencies, the Commission has made a number of strides with respect to managing its inventory and developing procedures. Our evaluation identified that the Commission needs to continue developing policies and procedures and ensure the implementation of those policies in a timely manner. Furthermore, the Commission needs to make improvements in the areas of vulnerability scanning, SA&A package development and Continuous Monitoring, as well as other areas such as, but not limited to training and testing for incident response and contingency planning.

The overall assessment of the Commission's information security program was deemed not effective because of the ratings throughout the IG FISMA Reporting Metrics domains, combined with the 11 findings, and associated 29 recommendations. The domain ratings are automatically scored when entered into CyberScope, and Level 4, Managed and Measurable, is considered to be an effective level of security at the domain, function, and overall program Level. OMB strongly encourages IGs to use the domain ratings to inform the overall Function ratings, and to use the five Function ratings to inform the overall agency rating.

CURRENT FINDINGS

The results our FISMA evaluation identified 11 findings related to FISMA controls, and these findings and the related 29 recommendations to remediate and/or enhance controls are detailed in the pages that immediate follow.

1. TIMELY REMEDIATION OF VULNERABILITIES

Condition:

Vulnerability scanning is not being conducted on a monthly basis, whereby vulnerabilities can be remediated timely. There has been scanning performed, however it is intermittent and there was no timely remediation of the identified vulnerabilities.

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:

The cause is primarily because of a lack of personnel, budget, or time constraints to adequately document and/or assess all of the controls in NIST 800-53, Revision 4.

Risk:

By having vulnerabilities (high and medium) exposed, and not remediated in a timely manner, there is the risk that adversaries can take advantage of those weaknesses and gain access to Commission 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 vulnerabilities or eliminating threats.

Recommendation(s):

1. The Office of Information Technology (OIT) should establish 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 business days.
2. The Commission should follow its vulnerability remediation policies.
3. 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.

Management's response:

Please refer to the Commission's response, included as **Attachment A**, which details management's planned action to implement a vulnerability remediation policy by January 31, 2018.

Auditor's comment to management's response:

The auditor maintains judgment that remediating high and moderate vulnerabilities according to the timelines recommended in this report are both necessary and reasonable under NIST 800-53, Revision 4. The timeframe referenced is to shed light upon the broader picture of industry best practices and not a comparison among agencies. The OIG plans to follow up on the Commission's implemented action to ensure the recommendations are fully addressed.

2. SA&A PACKAGE REQUIREMENTS

Condition:

The Commission does not have a completed Security Assessment & Authorization (SA&A) package for the GSS in scope. The required documents include the System Security Plan (SSP), Information System Contingency Plan (ISCP), Rules of Behavior (RoB), Security Assessment Report (SAR) and Plan of Actions and Milestones (POA&Ms) if there were any vulnerabilities which require remediation.

Criteria:

NIST 800-53 Revision 4, PL-2 states:

"Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions."

"The organization:

A. Develops a security plan for the information system that:

1. Is consistent with the organization's enterprise architecture;
2. Explicitly defines the authorization boundary for the system;
3. Describes the operational context of the information system in terms of missions and business processes;
4. Provides the security categorization of the information system including supporting rationale;
5. Describes the operational environment for the information system and relationships with or connections to other information systems;
6. Provides an overview of the security requirements for the system;
7. Identifies any relevant overlays, if applicable;
8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and
9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation."

NIST 800.53 Revision 4, PL-2 states:

CP-2 Contingency Planning

A. Develops a contingency plan for the information system that:

1. Identifies essential missions and business functions and associated contingency requirements;
2. Provides recovery objectives, restoration priorities, and metrics;
3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;

5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and

6. Is reviewed and approved by [Assignment: organization-defined personnel or roles].

NIST 800-53 Revision 4, PL-4 states:

"The organization:

A. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;

B. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;

C. Reviews and updates the rules of behavior [Assignment: organization-defined frequency]; and

D. Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated."

"(1) RULES OF BEHAVIOR | SOCIAL MEDIA AND NETWORKING RESTRICTIONS

The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites."

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 cause is primarily because of a lack of personnel, budget, or time constraints to adequately document and/or assess all of the controls in NIST 800-53.

Risk:

Without appropriately documenting the implementation of each of the control objectives, it will be unclear how specific controls are deployed. Without that clarity, controls may be deployed in a manner that is not commensurate with the risks of the system, which may expose the Commission to vulnerabilities and exploitation attempts. Without have a finalized ISCP, the Commission will be more exposed to risks in the event of an outage or disruption in operations. The Commission is not currently requiring personnel to have read, understood and agreed to the stipulations in the latest RoB, in accordance with NIST. This may lead to employees and/or contractors engaging in

activities that are adverse to the mission of the Commission and thereby expose the Commission to unforeseen risks. 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):

4. 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.
5. An ISCP should be developed, then reviewed and approved by the CIO, whereby all critical elements (hardware and software) are addressed in terms of their reconstitution of data.
6. The current RoB should be 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.
7. The Commission should identify any deficiencies (through the development of the SSP) and they should be documented on the SAR.
8. 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.
9. 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's response:

Please refer to the Commission's response, included as **Attachment A**, which details completed or initiated management actions to address some aspects of the recommendations.

Auditor's comment to management's response:

The auditor acknowledges some components of the SA&A package requirements as completed and pending further review. Based on the Commission's timely communication on the actions completed after the submission deadline in CyberScope application for October 31, 2017, the overall recommended actions for the SA&A package remains open, pending the completion for the ISCP scheduled for August 30, 2018. The OIG plans to follow up on the Commission's implemented actions to ensure the recommendations are fully addressed in the subsequent FISMA engagement.

3. PERSONNEL TERMINATION / TRANSFER

Condition:

Samples of two terminated users and two transferred users were tested to identify if their access rights were removed / updated within a timely manner. Upon review of the terminated users, there was no evidence that their access rights had been terminated within a timely manner.

After the fiscal year-end, it was revealed that the transferred users had been given increased job responsibilities so they were not required to have had their former access rights removed. However, there was no evidence that a review process was in place to determine whether the transferred users' rights should or should not be updated and, because of the lack of review, this is an issue.

Criteria:

NIST 800-53, Revision 4, Personnel Security (PS)-4 states:

"The organization, upon termination of individual employment:

A. Disables information system access within an organization-defined time period."

NIST 800-53, Revision 4, Personnel Transfer (PS)-5 states:

"The organization:

A. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization."

Cause:

The cause is primarily because of a lack of personnel, budget, or time constraints to adequately document and/or assess all of the controls in NIST 800-53, Revision 4.

Risk:

If the Commission has terminated or transferred users without having removed or updated their access in a timely manner, there is the risk that those users' accounts can be used for exploitation and adversarial actions against the Commission.

Recommendation(s):

10. The OIT should establish a formal policy and implement procedures for how timely separated and transferred users' access is removed or updated. Industry best practices are to remove separated users within 5 business days and updated transferred users within 5 business days.

Management's response:

Please refer to the Commission's response, included as **Attachment A**, which details management's planned actions for completion by January 30, 2018.

Auditor's comment to management's response:

The auditor acknowledges that management communicated the respective personnel security policy is in place after the submission deadline in CyberScope application for October 31, 2017. The OIG plans to follow up on the effectiveness on the Commission's implemented actions to ensure the recommendation is fully addressed.

4. PHYSICAL AND ENVIRONMENTAL CONTROLS

Condition:

Upon review of the server room, the following was observed:

- Badges were not required to gain entry into the server room.
- No video recording of the inside of the server room.
- No fire extinguisher.
- No automated notification of humidity levels.
- The main water line location was unknown.
- No emergency lighting.

Criteria:

NIST 800-53, Revision 4, Physical and Environmental Security (PE)-2 states:

"The organization:

A. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;

B. Issues authorization credentials for facility access;

C. Reviews the access list detailing authorized facility access by individuals [Assignment: organization-defined frequency]; and

D. Removes individuals from the facility access list when access is no longer required."

NIST 800-53, Revision 4, Physical and Environmental Security (PE)-10 states:

"The organization:

A. Provides the capability of shutting off power to the information system or individual system components in emergency situations;

B. Places emergency shutoff switches or devices in [Assignment: organization-defined location by information system or system component] to facilitate safe and easy access for personnel; and

C. Protects emergency power shutoff capability from unauthorized activation."

NIST 800-53, Revision 4, Physical and Environmental Security (PE)-13 states:

"The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source."

NIST 800-53, Revision 4, Physical and Environmental Security (PE)-14 states:

"The organization:

A. Maintains temperature and humidity levels within the facility where the information system resides at [Assignment: organization-defined acceptable levels]; and Monitors temperature and humidity levels [Assignment: organization-defined frequency]."

NIST 800-53, Revision 4, Physical and Environmental Security (PE)-15 states:

"The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel."

Cause:

The cause is primarily because of a lack of personnel, budget, or time constraints to adequately document and/or assess all of the controls in NIST 800-53, Revision 4.

Risk:

If the Commission has weak controls with regard to gaining access to the server room and/or inside the server room, there is an increased likelihood that the hardware supporting the Commission will either become compromised or damaged, thereby making the equipment inaccessible.

Recommendation(s):

11. The Commission should implement a process where 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).
12. Video monitoring should be occurring continuously without interruption inside the server room and the video should be maintained for at least one month before being overwritten.
13. Work with property management building 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.

Management's response:

Please refer to the Commission's response, included as **Attachment A**, which details management's planned action for completion by February 28, 2018.

Auditor's comment to management's response:

The auditor acknowledges management's response and risk-based decisions. The auditor was unable to provide humidity level readings because the server room does not have humidity detection and monitoring in place. Under NIST 800-53 Revision 4, the auditor applies discretion and judgment when selecting the controls to be evaluated. Our sample of controls were based upon interviews with management, risk to the Commission and maturity of the Commission's overall FISMA compliance. The OIG plans to follow up on the Commission's implemented actions to ensure the recommendations are fully addressed, in particular the fully integrated agency risk assessment that captures the taking of the risk decisions related to strategic planning, budgeting, and performance across IT activities.

5. CONTINGENCY TRAINING AND BACKUPS

Condition:

Although data is being backed up regularly, the backups are stored in the cloud with a third party provider, who is not FedRamp certified. It was also revealed that there is no contingency training provided for IT personnel. Moreover, as the ISCP has not been finalized, there has been no testing for contingencies (e.g. inadvertent shutdown, security incident preventing the access of critical data, etc.), in the event of a disaster.

Criteria:

NIST 800-53 Revision 4, CP-3 states:

"The organization provides contingency training to information system users consistent with assigned roles and responsibilities.

A. Within [Assignment: organization-defined time period] of assuming a contingency role or responsibility."

NIST 800-53 Revision 4, CP-4 states:

"The organization:

A. Tests and/or exercises the contingency plan for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests and/or exercises] to determine the plan's effectiveness and the organization's readiness to execute the plan."

NIST 800-53 Revision 4, CP-9 states:

"Protects the confidentiality, integrity, and availability of backup information at storage locations."

Cause:

The cause is primarily because of a lack of personnel, budget, or time constraints to adequately document and/or assess all of the controls in NIST 800-53, Revision 4.

Risk:

Without appropriately maintaining backup data at an external site, the Commission runs the risk that if the primary site has an adverse event (fire, flood, earthquake, theft, etc.) whereby the data is destroyed; the Commission will likely not be able to restore the data. If IT personnel have not received appropriate training with regard to handling a contingency or testing for contingencies, then there is an increased likelihood that if and when a disaster strikes, the Commission will be very unprepared and may suffer from loss of data.

Recommendation(s):

14. 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.
15. All IT personnel (both employees and contractors) should receive annual contingency training.
16. Once the ISCP is finalized, the ISCP should be tested annually to ensure that IT personnel are prepared for a disaster and back-ups are operational.

Management's response:

Please refer to the Commission's response, included as **Attachment A**, which details management's completion of planned actions by August 30, 2018.

Auditor's comment to management's response:

The auditor acknowledges management's efforts to have the data backed up regularly. The recommended action is to ensure the external service provider is FedRamp certified. The agency should be placing their data in an environment that meets or exceeds the NIST requirements.

Under NIST 800-53 Revision 4, the auditor applies discretion and judgment when selecting the controls to be evaluated. Our sample of controls were based upon interviews with management, risk to the Commission and maturity of the Commission's overall FISMA compliance. The OIG plans to follow up on the Commission's implemented actions to ensure the recommendations are fully addressed.

6. CONFIGURATION CHANGES

Condition:

Changes made to the GSS are not made in a controlled environment. The following was noted:

- A detailed listing of changes made during the prior year was not maintained.
- Formal approvals did not accompany the changes made.
- Formal testing with positive results were not maintained for each change.
- Subsequent auditing of changes was not conducted.

Criteria:

NIST 800-53, Revision 4, Configuration Management (CM)-3 states:

C. Documents configuration change decisions associated with the information system;

D. Implements approved configuration-controlled changes to the information system;

E. Retains records of configuration-controlled changes to the information system for [Assignment: organization-defined time period]; and

F. Audits and reviews activities associated with configuration-controlled changes to the information system."

"2. The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system."

Cause:

The cause is primarily because of a lack of personnel, budget, or time constraints to adequately document and/or assess all of the controls in NIST 800-53, Revision 4.

Risk:

If changes are made without appropriate approvals, testing (with positive results) or subsequent auditing, there is the risk that systems in production will have backdoors or possibly malicious code that can be exploited and harm the Commission.

Recommendation(s):

17. Establish and implement a process that documents all changes, with formalized approvals prior to the change, and captures evidence of the testing results.
18. Segregation of duties should exist between environments so that those making the changes are different from those personnel that approve the changes.
19. Each year, a sample of changes should be reviewed to ensure they comply with Commission procedures.

Management's response:

Please refer to the Commission's response, included as **Attachment A**, which details management's planned actions for completion by May 30, 2018.

Auditor's comment to management's response:

The actions described by the Commission are responsive to the recommendations. The OIG plans to follow up on the Commission's implemented actions to ensure the recommendations are fully addressed.

7. INCIDENT RESPONSE TRAINING AND TESTING

Condition:

Upon review of the incident response environment, the following was noted:

- It is necessary for agencies to test their Incident Response capabilities so that they can ensure there is proper handling of the respective incident (e.g. identifying if there is PII and then reporting to the US-CERT), management and response time, in the event of an incident. Although there is a formalized Incident Response Plan, this Plan was not tested to ensure that in the event of an incident, this Agency is prepared.
- There is also no training provided to the IT staff with respect to preparing for and/or managing incidents.
- The Incident Response Plan was not reviewed and updated annually.

Criteria:

NIST 800-53, Revision 4, Incident Response (IR)-2, training, states:

"The organization provides incident response training to information system users consistent with assigned roles and responsibilities."

NIST 800-53, Revision 4, Incident Response (IR)-3, testing, states:

"The organization tests the incident response capability for the information system to determine the incident response effectiveness and documents the results."

Cause:

The cause is primarily because of a lack of personnel, budget, or time constraints to adequately document and/or assess all of the controls in NIST 800-53, Revision 4.

Risk:

Without formalized and yearly testing and training on incident response, there is the risk that when an incident occurs, the Commission's response will be ineffective. This may also result in untimely remediation of the incident, thereby affecting Commission data and systems. In addition, there is the risk that the OIT and other staff members will be unprepared if and when an incident actually does occur.

Recommendation(s):

20. Test the Incident Response Plan annually, review the results and make updates as necessary.
21. All IT personnel (both employees and contractors) should receive incident response training annually.

Management's response:

Please refer to the Commission's response, included as **Attachment A**, which details management's planned actions for capturing updates by February 28, 2018, and training and testing efforts prior to August 30, 2018.

Auditor's comment to management's response:

The actions described by the Commission are responsive to both recommendations. The OIG plans to follow up on the Commission's implemented actions to ensure the recommendations are fully addressed.

8. ACCESS AUTHORIZATION MANAGEMENT

Condition:

Upon review of a sampled set of users for their access authorizations, the following was noted:

- Access authorizations are not being maintained to ensure that users' rights are commensurate with what was approved.
- There was no evidence to conclude that an annual recertification of users' access rights is being performed.
- Administrative (Admin) users are not being reviewed on a semi-annual basis.

Criteria:

NIST 800-53, Revision 4, Identification and Authorization (IA)-4 states:

"The organization manages information system identifiers [user accounts] by:

A. Receiving authorization from organization-defined personnel or roles to assign an individual, group, role, or device identifier." In addition, "The organization requires that the registration process to receive an individual identifier [user account] includes supervisor authorization."

NIST 800-53, Revision 4, Access Control (AC)-2 states:

"Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account."

"Authorizes access to the information system based on:

1. A valid access authorization;
2. Intended system usage; and
3. Other attributes as required by the organization or associated missions/business functions."

Cause:

The cause is primarily because of a lack of personnel, budget, or time constraints to adequately document and/or assess all of the controls in NIST 800-53, Revision 4.

Risk:

Without maintaining and reviewing users' access rights annually, there is the risk that users will be authorized for access levels in excess of the access levels they were approved for, thereby creating an environment where a user can potentially exploit the Commission's systems and data.

Recommendation(s):

22. All users' rights upon initiation should have their access rights reviewed, approved (by the respective employee's immediate supervisor), and maintained for subsequent investigations and/or incident response.
23. On an annual basis, all Commission employees should have their access reviewed (by the respective employee's immediate supervisor) to ensure it is still commensurate with their job functions.
24. On an annual basis, all admin users' accounts should be reviewed to ensure their authorizations are still appropriate.

Management's response:

Please refer to the Commission's response, included as **Attachment A**, which details management's planned actions to implement a process of the review on active accounts by March 30, 2018.

Auditor's comment to management's response:

The actions described by the Commission are responsive to the recommendations. The OIG plans to follow up on the Commission's implemented actions to ensure the recommendations are fully addressed.

9. COMPLEXITY SETTINGS

Condition:

Upon review of the configuration settings, the following was noted:

- Users are not automatically disabled after a period of 120 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 cause is primarily because of a lack of personnel, budget, or time constraints to adequately document and/or assess all of the controls in NIST 800-53, Revision 4.

Risk:

With users having no automated setting to automatically disable their user identification (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(s):

25. All users should have their IDs automatically disabled after a period of 120 days of inactivity.

Management's response:

Please refer to the Commissions response, included as **Attachment A**, which details management's planned action to implement policy by January 21, 2018.

Auditor's comment to management's response:

The action described by the Commission is responsive to the recommendation. The OIG plans to follow up on the Commission's implemented action to ensure the recommendation is fully addressed.

10. AUDIT EVENTS, REVIEWS, AND UPDATES

Condition:
Upon review and examination, the following was noted:

- The Windows server didn't have "Privileged Use", "Policy Change" or "Account Management" set to both success and failure.
- Audit logs are not currently being reviewed by anyone.

Criteria:
NIST 800-53 Revision 4, AU-2 states:

"Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents."

"(3) AUDIT EVENTS | REVIEWS AND UPDATES

The organization reviews and updates the audited events [Assignment: organization-defined frequency]."

Cause:
The cause is primarily because of a Congressional hold on providing tapes to external contractors. The cause is also due to a lack of understanding, as the Congressional hold should not prevent the Commission from protecting its data via the backup and storage at an off-site location.

Risk:
Without auditing privileged users, changing audit settings, or creating, modifying or deleting accounts, there is an increased likelihood that adverse actions will occur and there will be no detective controls in place to identify those actions.

Recommendation(s):

26. Audit settings should be updated so that "Privileged Use", "Policy Change", and "Account Management" are set to both success and failure.
27. Audit logs should be reviewed by both IT and management personnel within the Commission on a monthly basis and investigation or corrective action should take place accordingly.

Management's response:
Please refer to the Commission's response, included as **Attachment A**, which details management's response to implement planned actions by March 30, 2018.

Auditor's comment to management's response:
The actions described by the Commission are responsive to the recommendations. The OIG plans to follow up on the Commission's implemented actions to ensure the recommendations are fully addressed.

11. CONTINUOUS MONITORING

Condition:

Once a finalized SA&A package is complete, it is necessary to assess all of the NIST 800-53 controls over a three-year period, which is referred to as continuous monitoring. At the current time, there is no continuous monitoring being performed.

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."

Cause:

The cause is primarily because of a lack of personnel, budget, or time constraints to adequately document and/or assess all of the controls in NIST 800-53.

Risk:

Without testing all of the controls 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):

28. The Commission should identify the critical controls within NIST 800-53. Those critical controls should then be assessed and documented every year.
29. 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 1/3 of the controls are assessed. They should be assessed throughout the year as opposed to assessing the 1/3 controls at one time.

Management's response:

Please refer to the Commission's response, included as **Attachment A**, which details management's planned strategy to implement by April 30, 2018.

Auditor's comment to management's response:

The actions described by the Commission are responsive to the recommendations. The OIG plans to follow up on the Commission's implemented actions to ensure the recommendations are fully addressed.

ATTACHMENT A – COMMISSION'S RESPONSE

U.S. ABILITYONE COMMISSION

PHONE: 703-603-7740
FAX: 703-603-0655

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

November 30, 2017

Mr. Marcos Contreras
Assistant Inspector General for Auditing, AIGA
Office Of Inspector General (OIG), Audit Component
2331 Mill Road, Suite 505
Alexandria, VA 22314

Re: U.S. AbilityOne Commission FY 2017 FISMA Evaluation Report, AbilityOne Management Response to Audit Findings

Dear Mr. Contreras:

U.S. AbilityOne acknowledges receipt of the FY2017 FISMA Evaluation Report which identified eleven (11) findings. Our management responses are listed under each finding by title as referenced on the report. We identified a high level mitigation for each finding which is still outstanding along with an anticipated completion date for implementation of a remediation. Plan of action and milestones (POA&M) will be created to track progress of the open issues. Please reference the details below for information related to the findings from the FISMA report.

01 Timely Remediation of Vulnerabilities

AbiityOne concurs that this risk exists and will work towards establishing a routine scanning and remediation policy. AbilityOne does not agree with the auditor's recommendation regarding the short turnaround for remediation of vulnerabilities detected through scanning. The recommended remediation timeline would be burdensome for a micro/small agency and unwarranted for moderate to low risk data. AbilityOne's CIO and CISO will create a vulnerability remediation policy with agency defined timelines. The estimated completion date for the vulnerability remediation policy is January 31, 2018.

In the meantime, AbilityOne is requesting the auditor to elaborate on which industry standards and/or best practices (cite framework, paragraph, and sections) where this remediation timeframe is referenced.

02 SA&A Package Requirements

AbilityOne does have a System Security Plan which was completed and existed prior to the audit for FY2017. An annual security assessment was performed by an independent assessor, NIT, and a SA&A package was produced containing a Security Assessment Report (SAR), Plan of Actions and Milestones

(POA&Ms), Risk Assessment Report, FIPS 199, Security Control Assessment Report, and System Security Plan.

AbilityOne concurs that an Information System Contingency Plan (ISCP) is missing from its SA&A package. An Information System Contingency Plan (ISCP) will be completed by August 30, 2018.

AbilityOne does have a Rules of Behavior policy which includes restrictions for usage of social media, lasted updated on 9/15/2017 and approved by the CIO on 11/1/2017. The document is titled CBSD General Rules of Behavior for IT Users, September 15th 2017, Version 1.0.

03 Personnel Termination / Transfer

AbilityOne does have a Personnel Security Procedure "CBSD Personnel Security and Procedures V2-17.doc" which was last updated on 4/17/2017. This procedure requires that a terminated employee's access is removed within one day. AbilityOne's CIO and CISO will ensure a review and tracking mechanism is implemented to ensure the procedure is followed. This review process will be implemented by January 30, 2018.

04 Physical and Environmental Controls

AbilityOne acknowledges that its server room is located on the 7th Floor in a closet within the confined office suite of the agency's workers; therefore, this is a manageable risk due to not being a data center environment. AbilityOne does not have authorization to make mechanical, electrical, and plumbing modifications in a small office leased space. Access to the server room is via a cipher lock and only pertinent IT staff and management have access.

AbilityOne does not find the use of video monitoring necessary for reasons just noted in paragraph 1. Control PE-20 is not part of the control baseline for 800-53 rev 4. The controls scope on page 2 of the FISMA report needs adjusting to remove controls PE-18, PE-19, and PE-20.

AbilityOne will acquire a fire extinguisher and flashlights as emergency lighting for use in the computer closet by February 28, 2018.

AbilityOne notes that no humidity readings were provided by the auditor.

05 Contingency Training and Backups

AbilityOne currently has a data backup and management agreement with a reputable company, Baracuda. The data is backed up on a daily basis. AbilityOne will assess other cloud service providers for their backup services and compare.

AbilityOne concurs that it needs to develop an Information Security Contingency Plan (ISCP). Once the ISCP which is listed under finding number 2, SA&S Package Requirements, is completed, AbilityOne will incorporate training and testing exercises following completion of the plan. This training and testing will be completed by August 30, 2018.

The controls scope on page 2 of the FISMA report needs updating to remove controls CP-11 and CP-12 as they are not part of the control baseline for NIST 800-53 Rev 4.

06 Configuration Changes

AbilityOne concurs that there is an existing gap in its ability to test, track and implement changes. AbilityOne's CIO and CISO will review and update its configuration management policy and procedures to implement testing and configuration management tracking of changes. A security impact analysis will also be performed prior to implementation of changes. This process will be implemented by May 30, 2018.

07 Incident Response Training and Testing

AbilityOne does update its incident response plan annually. The CIO and CISO will implement a process to capture the plan updates history, training of staff, and testing of the incident response plan. The process for capturing updates will be implanted by Feb 28, 2018. The training of staff and testing of the incident response plan will occur prior to August 30, 2018.

08 Access Authorization Management

AbilityOne concurs with this finding. AbilityOne currently has an Identification and Authentication Procedure which indicates that the activity in this finding would and should be performed. AbilityOne's CIO and CISO will implement a process to review active accounts on a semi-annual basis. This process will be implemented and the subsequent review performed by March 30, 2018.

09 Complexity Settings

AbilityOne acknowledges that this finding was an issue at the time of the audit. AbilityOne has manually disabled accounts which were previously inactive for over 120 days. AbilityOne will implement policy to automatically disable accounts after 120 days of inactivity. This policy will be implemented by January 21, 2018.

10 Auditing

AbilityOne acknowledges that the Windows server settings for "Privileged Use" and "Policy Chance" were not set to record Failure and Success at the time of the audit; however, the settings have now been updated to record both results. This portion of the finding has been resolved.

Audit logs will be reviewed by the CISO on a quarterly basis at a minimum. This practice will be implemented by March 30, 2018.

11 Continuous Monitoring

AbilityOne hired an independent assessor, NIT, who performs an assessment of its security controls on an annual basis. The SA&A package for FY2017 existed at the time of the audit. This portion of the finding is resolved.

AbilityOne's CIO and CISO will create a continuous monitoring strategy and subsequently a Security Control Traceability Matrix (SCTM) to identify controls and facilitate the tracking of control status. Cycles of control reviews will occur throughout each year to account for the total control baseline. The overall continuous monitoring strategy and SCTM will be created and implemented by April 30, 2018.

Sincerely,

Michael J. Rogers
Chief of Staff
U.S. AbilityOne Commission