Office of Inspector General

Committee for Purchase From People Who Are Blind or Severely Disabled (U.S. AbilityOne Commission)

November 21, 2019

MEMORANDUM

FOR: Thomas D. Robinson
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. 20-01

I am pleased to provide as required by the Federal Information Security Modernization Act of 2014 (P.L. 113-283), the results of the annual independent evaluation of the Commission's Information Security Program and Practices for Fiscal Year (FY) 2019.

The Office of Inspector General (OIG) contracted with McConnell & Jones LLP, an independent public accounting (IPA) firm, to conduct this independent evaluation. McConnell & Jones served as the auditor and the OIG monitored the contractor's performance.

The objective of the evaluation was to assess the effectiveness of the Commission's information security and privacy program as of September 30, 2019. The scope of this evaluation focused on the Commission's General Support System (GSS) and related information security policies, procedures, standards, and guidelines. The evaluation assessed the Commission's maturity level across key areas and its compliance using the evaluation guide developed by the Council of the Inspectors General on Integrity and Efficiency (CIGIE).

The overall assessment of the Commission's FY 2019 information security program was deemed not effective because the tested, calculated and assessed maturity levels across the functional and domain areas received an overall rating at Level 3 – Consistently Implemented. The findings from the evaluation demonstrate that improvements are needed with respect to continuous monitoring and information system and communication.

The Commission concurred with all three recommendations, and for the purpose of this public version report, their comments are summarized within the body of the report as appropriate.

The Commission received the report with complete details on the findings and recommendations to address the information security and technology improvements needed.

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: Tina Ballard, Executive Director
Kelvin Wood, Chief of Staff
Edward Yang, Chief Information Officer

Executive Summary, Report No. 20-01, November 21, 2019
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 not effective because the tested, calculated and assessed maturity levels across the functional and domain areas received an overall rating at Level 3 – Consistently Implemented. At this level, the Commission took positive steps to implement policies, procedures and strategies; however, the Commission needs to ensure implemented actions are assessed over time to make appropriate adjustments as needed.

The two findings from the evaluation demonstrate that improvements are needed with continuous monitoring, and information system and communication.

Recommendations

The report contains three recommendations, when implemented, those actions should strengthen the IT system operations and assist the Commission with FISMA compliance requirements.

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

Objective

In accordance with FY 2019 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. The FY 2019 IG FISMA Reporting Metrics reflected the collaborative effort amongst 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 align with the Cybersecurity Framework function areas and maturity model indicators.

Office of the Inspector General

for

U.S. AbilityOne Commission

FY 2019 Evaluation of the U.S. AbilityOne Commission's Compliance with the Federal Information Security Modernization Act

November 21, 2019

FINAL REPORT – REDACTED FOR PUBLIC RELEASE

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

November 21, 2019

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) 2019. 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'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' generals 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 an information security program of an agency. The overall assessment of the Commission's FY 2019 information security program was deemed not effective because the tested, calculated and assessed maturity levels across the functional and domain areas received an overall rating at Level 3 – Consistently Implemented. 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 three new recommendations in this year's evaluation. The Commission's comments are summarized within our report.

McConnell & Jones would like to thank the Office of the Inspector General (OIG) and the Commission's Information Technology (IT) Staff for their assistance in helping us meet the objective of our evaluation.

McConnell Jones LLP

McConnell & Jones LLP

Table of Contents

SECTION **PAGE NUMBER**

Executive Summary

Pursuant to the Federal Information Modernization Act (FISMA), the U.S. AbilityOne Commission Office of Inspector General (OIG) engaged McConnell & Jones to conduct the annual evaluation and complete the fiscal year (FY) 2019 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, 2019.

In accordance with FISMA and Office of Management and Budget (OMB) Memorandum M-19-02, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*, the OIG submitted the IG FISMA Reporting Metrics into the Department of Homeland Security's (DHS) CyberScope application on October 31, 2019. The Commission made progress through consistent implementation of security policies, procedures, and strategies, but lacked quantitative and qualitative measures to assess them and make necessary changes.

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 2019 information security program was deemed not effective because the tested, calculated and assessed maturity levels across the functional and domain areas received an overall rating at Level 3 – Consistently Implemented.

The Commission implemented all 29 recommendations from the prior years' evaluations. 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. Our findings and recommendations will improve the Commission's IT security and privacy operations and its compliance with FISMA functional areas.

In order to ensure the safety and security of the Commission's information system and communication, we determined Finding 2 and associated recommendation require redaction from public release. The Commission received the full version of this report (full version report) that includes the details and recommended action to address Finding 2. The Commission's management and IT staff remain responsible for following-up on all the 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 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 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.

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, 2018 through September 30, 2019 (FY 2019).

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 2019 FISMA evaluation, we reviewed 14 control families and 34 associated controls. The full version report issued to the Commission includes the scope of our testing of new controls, along with testing of the controls from the prior year.

[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 2019 FISMA evaluation identified two findings related to the FISMA controls evaluated, and we provided three recommendations.

01. Continuous Monitoring

Condition:

Once a finalized Security Assessment and Authorization (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 Commission is running scans within NIST 800-53, but the scans failed to capture all of the controls referred to as continuous monitoring.

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):

1. The Commission should identify the critical controls within NIST 800-53. Those critical controls should then be assessed and documented every year.
2. 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 Response:

The Commission concurred with the finding and recommendations. Management's comments are included in the full version report issued to the Commission which details management's planned actions for completion by December 31, 2019.

Auditor's Response to Management's Comments

The comments from the Commission were generally responsive to our findings and recommendations. As noted in recommendation numbers 1 and 2, the Commission's responses indicate the selection of critical control families, rather than identifying the specific/associated controls within those families. Management needs to ensure that the specific controls in each family are identified to address the intent of each recommendation.

Finding 1, Recommendation No. 1

Our recommendation addresses the identification of critical controls within NIST 800-53, and having those controls assessed and documented every year. Although management identified six control families, the specific/associated controls were not identified. Furthermore, the annual assessment and documentation will require additional time to implement and fully complete this action. Management retains the responsibility to ensure the complete list of families and controls are documented and assessed annually as part of the Commission's Information System Continuous Monitoring (ISCM). The OIG plans to follow up on the Commission's implementation action to ensure the recommendation is fully addressed.

Finding 1, Recommendation No. 2

Our recommendation addresses the identification of the remaining controls in NIST 800-53 (all controls less than critical controls), and assessment over a three-year period with a methodology to evaluate 1/3rd annually. The identification should include the specific/associated controls within the control families provided in the Commission's response. Furthermore, the assessment over the three-year period, and the 1/3rd of controls assessed yearly will take time to complete and reflect full implementation of actions. The OIG plans to follow up on the Commission's implementation to ensure the recommendation is fully addressed.

02. Information System and Communication

We provided the complete details of the finding and recommendation to address information system and communication weaknesses in the report issued to the Commission. The Commission concurred with the recommendation and management comments were attached to the report provided to the Commission. No further details are contained within this public version report.

Prior Year Findings

During the FY 2019 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 recommendations.

The FY 2017 IG FISMA evaluation contained 11 findings and 29 associated recommendations. During FY 2018, the Commission remediated and closed 25 of 29 recommendations. The Commission implemented the remaining 4 recommendations later in 2018 and they have been closed during 2019 based upon analysis and testing performed to assess remediation.

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 four prior years' open recommendations which have been closed during FY 2019:

FY 2017 FISMA RECOMMENDATIONS CLOSED DURING FY 2019

Status of Recommendations	Year / Rec. #	Status
Timely Remediation of Vulnerabilities		
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	Closed
SA&A Package Requirements		
The System Security Plan (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	Closed
Contingency Training and Backups		
IT should store incremental and full back-ups offsite. If backups are to be stored with a third-party provider, then this vendor must be FedRamp certified.	2017 – 14	Closed
Configuration Changes		
Each year, a sample of changes should be reviewed to ensure they comply with Commission procedures.	2017 – 19	Closed