OFFICE OF INSPECTOR GENERAL

THE MILLENNIUM CHALLENGE CORPORATION HAS IMPLEMENTED MANY CONTROLS IN SUPPORT OF FISMA, BUT IMPROVEMENTS ARE NEEDED

AUDIT REPORT NO. A-MCC-17-003-C
NOVEMBER 7, 2016

WASHINGTON, DC

Please note that certain information contained in this transmittal memo and attached report has been redacted as "SBU" (sensitive but unclassified) by MCC officials, meaning that public disclosure of this material could compromise the integrity of government computer systems and networks. All redactions are made under Freedom of Information Act Exemption 7(E).

Office of Inspector General

November 7, 2016

Mr. Vincent Groh
Chief Information Officer
Millennium Challenge Corporation
1099 Fourteenth Street, NW
Washington, DC 20005

Dear Mr. Groh:

Enclosed is the final report, "The Millennium Challenge Corporation Has Implemented Many Controls in Support of FISMA, but Improvements Are Needed" (A-MCC-17-003-C). The Office of Inspector General (OIG) contracted with the independent certified public accounting firm of CliftonLarsonAllen LLP (Clifton) to conduct the audit.

In carrying out our oversight responsibilities, we reviewed Clifton's report and related audit documentation. Our review was different from an audit in accordance with U.S. generally accepted government auditing standards and was not intended to enable us to express, and we do not express, an opinion on the Millennium Challenge Corporation's (MCC) compliance with the Federal Information Security Modernization Act of 2014 (FISMA). Clifton is responsible for the enclosed auditor's report and the conclusions expressed in it. We found no instances of Clifton not complying, in all material respects, with applicable standards. According to Clifton officials, they performed the audit in accordance with U.S. generally accepted government auditing standards.

The audit objective was to determine whether MCC implemented selected security controls for selected information systems in support of FISMA. To answer the audit objective, Clifton tested MCC's implementation of selected controls outlined in National Institute of Standards and Technology Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations." The audit included five MCC-managed information systems: MCCNet general support system, MCC Public Website, MCC Management Information System, MCA Collaborate, and Contract Management System Audit Tracking and Reporting System. Clifton conducted fieldwork at MCC's headquarters in Washington, DC, from March 28, 2016, through July 22, 2016.

Clifton concluded that MCC implemented 85 of 102 selected security controls for selected information systems in support of FISMA. However, MCC did not implement 17 controls designed to preserve the confidentiality, integrity, and availability of the information in its information systems. Therefore, Clifton concluded that, because of these weaknesses, MCC's information systems are at risk of unauthorized access, use, disruption, modification, and destruction, and its information is at risk of disclosure.

MCC complied with requirements including the following:

- Implemented an effective program for incident handling and response.
- Maintained an adequate and effective specialized training program for its employees requiring role-based training.
- Implemented an effective vulnerability identification process.
- Implemented effective audit log monitoring, review, and analysis.

However, MCC still needs to do the following:

- Strengthen security controls for patch and configuration management.
- Strengthen account management controls for the Contract Management System Audit Tracking and Reporting System.
- Strengthen physical and environmental controls for the secondary data center.
- Strengthen configuration management procedures.
- Document and implement policy and procedures for personnel security.
- Implement information system agreements for all external systems.
- Strengthen personnel out-processing procedures.
- Fully implement multifactor authentication for all network accounts.
- Update system inventory to include contractor management systems.

To address the weaknesses reported by Clifton, we make the following recommendations to MCC's management.

Recommendation 1. *We recommend that Millennium Challenge Corporation's Chief Information Officer document and implement a process to update baseline configurations for workstations periodically or document acceptance of the risk.*

Recommendation 2. *We recommend that Millennium Challenge Corporation's Chief Information Officer implement written procedures to complete, approve, and maintain users' access request forms for the Contract Management System Audit Tracking and Reporting System in accordance with "MCC Access Control Procedures."*

Recommendation 3. *We recommend that Millennium Challenge Corporation's Chief Information Officer either implement environmental controls for the secondary data center and document results or document acceptance of the risk.*

Recommendation 4. *We recommend that Millennium Challenge Corporation's Chief Information Officer document and implement a written physical and environmental protection policy that includes all security controls required by National Institute of Standards and Technology Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," and reflects the current operating environment.*

Recommendation 5. *We recommend that Millennium Challenge Corporation's Chief Information Officer document and implement written procedures to manage access to the secondary data center. At a minimum, the procedures should include periodically reviewing logs of personnel entering the data center, and implementing a visitor access log for the data center.*

Recommendation 6. *We recommend that Millennium Challenge Corporation's Chief Information Officer activate the alarm in the secondary data center and document the results.*

Recommendation 7. *We recommend that Millennium Challenge Corporation's Chief Information Officer update the written "Configuration Management Policies and Procedures" to include testing and approval requirements by each type of system change.*

Recommendation 8. *We recommend that Millennium Challenge Corporation's Chief Information Officer document and implement policy and procedures that include all personnel security controls required by National Institute of Standards and Technology Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations."*

Recommendation 9. *We recommend that Millennium Challenge Corporation obtain a written, fully executed interconnection security agreement with the U.S. Department of Interior's Interior Business Center.*

In finalizing the report, Clifton evaluated MCC's responses to recommendations 1 through 9 in the draft report. Both Clifton and OIG acknowledge MCC's management decisions on all nine recommendations.

We appreciate the cooperation and courtesies you extended to our staff and Clifton's employees during the engagement.

Sincerely,

/s/
Alvin A. Brown
Deputy, Assistant Inspector General for Audit

The Millennium Challenge Corporation Has Implemented Many Controls in Support of FISMA, But Improvements Are Needed

Fiscal Year 2016

Final Report

4250 N. Fairfax Drive
Suite 1020
Arlington, Virginia 22203
tel: 571-227-9500
fax: 571-227-9552
www.claconnect.com

TABLE OF CONTENTS

Summary of Results 1

Audit Findings 3

MCC Needs to Strengthen Security Controls Surrounding Patch and Configuration Management 3

Account Management Controls Need to be Strengthened for the Contract Management System Audit Tracking and Reporting System 4

Environmental Controls Surrounding the Secondary Data Center Need Improvement 5

Physical Access Controls Surrounding the Secondary Data Center at the Headquarters Building Need Improvement 6

MCC Needs to Strengthen Configuration Management Procedures 8

Personnel Security Control Policy and Procedures Need to be Documented and Implemented 9

External Information System Agreements Need to be Current 10

MCC Needs to Strengthen Personnel Out-Processing Procedures 10

MCC Needs to Fully Implement Multifactor Authentication for all Network Accounts 11

Information System Inventory Needed to be Updated 12

Evaluation of Management Comments 13
Appendix I – Scope and Methodology 14
Appendix II – Management Comments 16
Appendix III – Status of Prior Year Findings 19
Appendix IV – Summary of Results of Each Control Reviewed 21

SUMMARY OF RESULTS

The Federal Information Security Modernization Act of 2014[1] (FISMA), requires federal agencies to develop, document, and implement an agency wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other source. Because the Millennium Challenge Corporation (MCC) is a federal agency, it is required to comply with federal information security requirements.

The act also requires agency heads to ensure that (1) employees are sufficiently trained in their security responsibilities, (2) security incident response capability is established, and (3) information security management processes are integrated with the agency's strategic and operational planning processes. All agencies must also report annually to the Office of Management and Budget and Congressional committees on the effectiveness of their information security program. In addition, FISMA has established that the standards and guidelines issued by the National Institute of Standards and Technology are mandatory for Federal agencies.

The USAID Office of Inspector General engaged us, CliftonLarsonAllen LLP, to conduct an audit in support of the FISMA requirement for an annual evaluation of MCC's information security program. The objective of this performance audit was to determine whether MCC implemented selected security controls for selected information systems[2] in support of FISMA.

Our audit was performed in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We audited 5 of the 6 systems in MCC's systems inventory as of May 2016, as follows: (1) MCCNet general support system; (2) MCC Public Website; (3) MCC Management Information System (MCC MIS); (4) MCA Collaborate; and (5) Contract Management System Audit Tracking and Reporting System.

Results

The audit concluded that MCC generally complied with FISMA requirements by implementing 85 of 102 selected security controls[3] for selected information systems. For example, MCC complied with the following requirements:

[1] The Federal Information Security Modernization Act of 2014 (Public Law 113–283—December 18, 2014) amends the Federal Information Security Management Act of 2002 to: (1) reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices, and (2) set forth authority for the Secretary of the Department of Homeland Security to administer the implementation of such policies and practices for information systems.

[2] See Appendix IV for a list of systems and controls selected.

[3] See Appendix IV – Summary of Results of Each Control Reviewed.

- Implementing an effective incident handling and response program.
- Maintaining an adequate and effective specialized training program for its employees requiring role-based training.
- Implementing an effective vulnerability identification process.
- Implementing effective audit log monitoring, review and analysis.

Although MCC generally had policies for its information security program, its implementation of those policies for 17 of the 102 selected controls was not fully effective to preserve the confidentiality, integrity, and availability of the corporation's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. Consequently, the audit identified areas in MCC's information security program that needed to be improved. Specifically, MCC needed to:

- Strengthen security controls surrounding patch and configuration management.
- Strengthen account management controls for the Contract Management System Audit Tracking and Reporting System.
- Strengthen physical and environmental control surrounding the secondary data center.
- Strengthen configuration management procedures.
- Document and implement personnel security policy and procedures.
- Implement information system agreements for all external systems.
- Strengthen personnel out-processing procedures.
- Fully implement multifactor authentication for all network accounts.
- Update its system inventory to include contractor-managed systems.

Consequently, MCC's operations and assets are at risk of unauthorized access, misuse and disruption. We made nine recommendations to assist MCC in strengthening its information security program. (See pages 3 – 12.)

Detailed findings appear in the following section. Appendix I describes the audit scope and methodology.

In response to the draft report, MCC outlined and described its plans to address all nine audit recommendations. Based on our evaluation of management comments, we acknowledge management decisions on all recommendations. MCC's comments are included in their entirety in Appendix II (pages 16 – 18).

AUDIT FINDINGS

1. MCC Needs to Strengthen Security Controls Surrounding Patch and Configuration Management

~~(SBU)~~ National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, security control [redacted] states the following regarding [redacted]:

> The organization [redacted]

~~(SBU)~~ In addition, security control [redacted]:

> The organization:
>
> * * *
>
> [redacted]

~~(SBU)~~ MCC did not [redacted]. Specifically, MCC [redacted] and relied on [redacted] to [redacted] with the [redacted] MCC indicated it would not be feasible to create a [redacted] specifically to [redacted] and [redacted] to the [redacted]. As a result, [redacted] such as those [redacted]. Specifically, [redacted] were both [redacted]

~~(SBU)~~ MCC management indicated the [redacted] were [redacted] because the [redacted] had not been [redacted]. MCC management also indicated that [redacted], which had not [redacted] since they had not been [redacted].

[4] [redacted]

~~(SBU)~~ By not [redacted] MCC is at a [redacted]. For example:

- [redacted].
- MCC employees may be [redacted].
- MCC [redacted]

Recommendation 1: *We recommend that the Millennium Challenge Corporation's Chief Information Officer document and implement a process to update baseline configurations for workstations on an corporation-defined periodic basis or document acceptance of the risk.*

2. Account Management Controls Need to be Strengthened for the Contract Management System Audit Tracking and Reporting System

(SBU) NIST Special Publication 800-53, Revision 4, security control [redacted], states the following regarding account management:

> The organization [redacted]

(SBU) In addition, *MCC Access Control Procedures*, dated March 16, 2016, states:

> [redacted]

(~~SBU~~) [redacted] as required by policy. Specifically, of the 88 [redacted], 14 of a sample of 14 [redacted]. Management indicated that [redacted]. Management will [redacted].

(SBU) By not ensuring that [redacted]. As a result, we recommend the following:

Recommendation 2: *We recommend that the Millennium Challenge Corporation's Chief Information Officer implement written procedures to complete, approve, and maintain access request forms for users with access to the Contract Management System Audit Tracking and Reporting System in accordance with policies.*

3. Environmental Controls Surrounding the Secondary Data Center Need Improvement

~~(SBU)~~ NIST Special Publication 800-53, Revision 4, controls state the following regarding

The organization:

The organization

Controls
The organization:

~~(SBU)~~ MCC's at the as the however, the did not have . Specifically, we noted the following:

- The did not have
- were not maintained for the
- were not present in the .
- There were no defined and for the and the and were not .

(SBU) Management indicated that the current the to by August 31, 2016.

~~(SBU)~~ Once the [redacted], the [redacted] be a [redacted], and the [redacted] will meet all the requirements for [redacted].

~~(SBU)~~ By not ensuring adequate [redacted], management may not be able to [redacted] in the [redacted] of a [redacted]. In addition, without the [redacted], there is an increased risk of potential [redacted]. As a result, we recommend the following:

> ***Recommendation 3:*** *We recommend that the Millennium Challenge Corporation's Chief Information Officer either implement environmental controls for the secondary data center and document results or document acceptance of the risk.*

4. Physical Access Controls Surrounding the Secondary Data Center at the Headquarters Building Needs Improvement

~~(SBU)~~ NIST Special Publication 800-53, Revision 4, [redacted] controls state the following regarding [redacted] controls:

> [redacted]
>
> The organization:
>
> * * *
>
> c. [redacted] and
>
> [redacted]
>
> The organization:
>
> * * *
>
> [redacted]

The organization:

~~(SBU)~~ Controls were not adequate to ensure appropriate Specifically, we noted the following:

- Management of personnel. In addition, a defined for
- and . Management did not have a in place to
- were not maintained for the .
- The within the had not been .

~~(SBU)~~ Management indicated that the was a by August 31, 2016. Once be a , and the will meet all the requirements .

~~(SBU)~~ In addition, a was not formally documented for the MCC's and . MCC did have a however, the was not the . Specifically, the policy defined Furthermore, the identified in NIST 800-53, Revision 4, related to the .

~~(SBU)~~ Weak controls over MCC systems increase the risk of individuals gaining unauthorized access to MCC systems and data. In addition, weak controls over can increase the risk of individuals gaining and disrupting MCC operations. As a result, we recommend the following:

> ***Recommendation 4:*** *We recommend that the Millennium Challenge Corporation's Chief Information Officer document and implement a written physical and environmental protection policy that addresses all required security controls as required by National Institute of Standards and Technology Special Publication 800-53, Revision 4,* Security and Privacy Controls for Federal Information Systems and Organizations *and reflects the current operating environment.*

Recommendation 5: *We recommend that the Millennium Challenge Corporation's Chief Information Officer document and implement written procedures to manage access to the secondary data center. At a minimum, the procedures should cover periodically reviewing access to the data center, reviewing access logs of personnel accessing the data center, and implementing a visitor access log for the data center.*

Recommendation 6: *We recommend that the Millennium Challenge Corporation's Chief Information Officer activate the alarm within the secondary data center and document the results.*

5. MCC Needs to Strengthen Configuration Management Procedures

NIST Special Publication 800-53, Revision 4, security control CM-3, states the following regarding configuration change control:

> The organization:
> a. Determines the types of changes to the information system that are configuration controlled;
> b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses.
> * * *

In addition, security control CM-9, states the following regarding configuration management plan:

> The organization develops, documents, and implements a configuration management plan for the information system that:
> a. Addresses roles, responsibilities, and configuration management processes and procedures;
> b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
> c. Defines the configuration items for the information system and places the configuration items under configuration management.

Of the 146 MCCNet change requests for fiscal year 2016, 3 of the 15 sampled requests did not have evidence of approval by MCC's change control board. Management indicated that these changes were routine and did not require change control board approval. However, MCC's *Configuration Management Policy and Procedures* did not establish the business rules by which changes were made and when change control board approval was not needed.

Without proper approvals of system changes, security deficiencies and vulnerabilities may exist that go undetected and unauthorized changes may be implemented. As a result, we are recommending the following:

Recommendation 7: *We recommend that the Millennium Challenge Corporation Chief Information Officer update the written C*onfiguration Management Policies and Procedures *to include testing and approval requirements by the type of system changes.*

6. Personnel Security Control Policy and Procedures Need to be Documented and Implemented

~~(SBU)~~ NIST Special Publication 800-53, Revision 4, security control [redacted], states the following regarding [redacted] policy and procedures:

> The organization:
> a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
>
> [redacted]

~~(SBU)~~ MCC did not have a [redacted] policy and procedures in place that encompasses all [redacted] controls as outlined in NIST Special Publication 800-53, Revision 4. The current policy in place is the [redacted] which only focuses on [redacted] requirements. However, it does not address policies and procedures relating to [redacted]. MCC had just focused the policy on [redacted] and is currently in the process of creating a policy that will supersede the current policy in place to address all required [redacted] controls.

~~(SBU)~~ Without current [redacted] policies and procedures to reflect current security control standards and environment, MCC may not be adequately implementing the associated [redacted] controls. As a result, we recommend the following:

Recommendation 8: *We recommend that the Millennium Challenge Corporation's Chief Information Officer document and implement a personnel security policy and procedures that addresses all applicable personnel security controls as required by National Institute of Standards and Technology Special Publication 800-53, Revision 4,* Security and Privacy Controls for Federal Information Systems and Organizations*.*

7. External Information System Agreements Need to be Current

NIST Special Publication 800-53, Revision 4, security control CA-3, states the following regarding system interconnections:

> The organization:
> * * *
> b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and
> c. Reviews and updates the Interconnection Security Agreements [Assignment: organization-defined frequency].

The Interconnection Security Agreement (ISA) between MCC and the Department of Interior (DOI) Interior Business Center (IBC) expired April 30, 2016. This agreement addresses the interconnection between the two parties' networks for the purposes of providing MCC's users with access to the IBC's Travel, Human Resources, and Oracle Federal Financials systems and the connections within the MCC network. MCC sent the final draft of the ISA to DOI for final review and signature but the final official signed copy was not returned to MCC.

Without an agreement, security controls that will be in place to protect the confidentiality, integrity, and availability of the DOI/IBC and MCC systems and the data transferred between them are not documented, increasing the risk that adequate security over MCC data will not be implemented. In addition, when system interfaces are not accurately understood and documented, there is an increased risk that data may be added, lost, or altered during processing.

> ***Recommendation 9:*** *We recommend that the Millennium Challenge Corporation obtain a written, fully executed Interconnection Security Agreement with the Department of Interior's Interior Business Center.*

8. MCC Needs to Strengthen Personnel Out-Processing Procedures

NIST Special Publication 800-53, Revision 4, security control PS-4, states the following regarding personnel termination:

> The organization, upon termination of individual employment:
> * * *
> f. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].

Of the 60 terminated personnel in fiscal year 2016, MCC did not maintain exit forms for a sample of five. Neither MCC's Chief of Information Security staff nor its Office of Domestic and International Security was able to retrieve the exit forms. MCC is working on a new ticketing system to ensure exit checklist are being completed and access is properly terminated with an anticipated completion dated of September 30, 2016. However, the control was not implemented at the time of the audit.

If the employee separation process is not completed properly; including completion of all necessary documentation, collection of all organization property (badges, keys, keycards, etc.), and revocation of all employee access; MCC's security as well as information integrity may become compromised.

A recommendation addressing this finding was made in the fiscal year 2015 audit;[5] however, procedures were not fully implemented and MCC did not close the recommendation. Therefore, we are not making additional recommendations at this time.

9. MCC Needs to Fully Implement Multifactor Authentication for all Network Accounts

~~(SBU)~~ According to NIST Special Publication 800-53, Revision 4, security control [redacted] the organization should implement [redacted]

~~(SBU)~~ In addition, [redacted]

~~(SBU)~~ MCC did not implement [redacted] MCC uses the [redacted] However, MCC's [redacted] issue contractors [redacted] until the system is upgraded. Delays for the system upgrade have extended over a year while the [redacted] completed an authorization to operate for the upgraded system. Therefore, MCC has to send its contractors to [redacted] but it is a slow process. MCC plans to implement a new system by July 2016 and implement [redacted] by the end of fiscal year 2016.

~~(SBU)~~ By not implementing [redacted] MCC increases the risk that unauthorized individuals could gain access to its information system and data.

A recommendation addressing this finding was made in the fiscal year 2015 audit;[6] however, procedures were not fully implemented and MCC did not closed the recommendation. Therefore, we are not making additional recommendations at this time.

[5] Recommendation 2, *Audit of the Millennium Challenge Corporation's Fiscal Year 2015 Compliance with the Federal Information Security Management Act of 2002, As Amended* (Audit Report No. A-MCC-16-001-P, October 26, 2015).

[6] Recommendation 6, *Audit of the Millennium Challenge Corporation's Fiscal Year 2015 Compliance with the Federal Information Security Management Act of 2002, As Amended* (Audit Report No. A-MCC-16-001-P, October 26, 2015) .

10. Information System Inventory Needed to be Updated

The Federal Information Security Management Act of 2002 states the following regarding information system inventory:

> c) Inventory of Major Information Systems.—
> (1) The head of each agency shall develop and maintain an inventory of major information systems (including major national security systems) operated by or under the control of such agency.
> (2) The identification of information systems in an inventory under this subsection shall include an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency.
> (3) Such inventory shall be—
> (A) updated at least annually.

The MCC information system inventory was not up-to-date and accurately described. Specifically, the information system inventory did not include contractor-operated systems that were being used by MCC or that maintain MCC data. These included the eOPF, FedHR Navigator, IBCNet, USAID Network, and e-Travel systems. The IBCNet system includes the following applications:

- iProcurement
- Federal Personnel Payroll System
- Quicktime
- Oracle Federal Financials

Management was not aware of the FISMA requirement for the system inventory to include systems not operated by or under the control of the corporation.

Without an up-to-date and accurate inventory of information systems, there is an increased risk that security controls will not be appropriately implemented and monitored for all systems. Upon notification of the issue, MCC took action to correct this weakness. Therefore, we are not making a recommendation at this time.

EVALUATION OF MANAGEMENT COMMENTS

In response to the draft report, the Millennium Challenge Corporation (MCC) outlined its plans to address all nine recommendations and described planned actions to address the recommendations. MCC's comments are included in their entirety in Appendix II.

Based on our evaluation of management comments, we acknowledge management decisions on all nine recommendations.

APPENDIX I

SCOPE AND METHODOLOGY

Scope

We conducted this audit in accordance with generally accepted Government auditing standards, as specified in the Government Accountability Office's Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. The audit was designed to determine whether MCC implemented selected security controls for selected information systems[7] in support of the Federal Information Security Modernization Act of 2014.

The audit included the testing of selected management, technical, and operational controls outlined in National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.* We assessed MCC's performance and compliance with FISMA in the following areas:

- Access Controls
- Audit and Accountability
- Awareness and Training
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Personnel Security
- Physical and Environmental Controls
- Program Management
- Risk Assessment
- Security Assessment and Authorization
- System and Communications Protection
- System and Information Integrity
- System and Service Acquisition

For this audit, we reviewed the 5 of the 6 systems in MCC's inventory as of May 2016: (1) MCCNet general support system; (2) MCC Public Website; (3) MCC Management Information System (MCC MIS); (4) MCA Collaborate; and (5) Contract Management System Audit Tracking and Reporting System. See Appendix IV for a listing of selected controls for each system. The audit also included a vulnerability assessment of MCC's general support system and an evaluation of MCC's process for identifying and

[7] See Appendix IV for a list of systems and controls selected.

correcting/mitigating technical vulnerabilities. The audit also included a follow up on prior audit recommendations[8] to determine if MCC made progress in implementing the recommended improvements concerning its information security program.

The audit fieldwork was performed at the Millennium Challenge Corporation's headquarters in Washington, D.C., from March 28, 2016, to July 22, 2016.

Methodology

To determine if MCC's information security program met FISMA requirements, we conducted interviews with MCC officials and contractors and reviewed legal and regulatory requirements stipulated in FISMA. We also reviewed documents supporting the information security program. These documents included, but were not limited to, MCC's (1) information security policies and procedures; (2) incident response policies and procedures; (3) access control procedures; (4) patch management procedures; and (5) change control documentation. Where appropriate, we compared documents, such as MCC's information technology policies and procedures, to requirements stipulated in National Institute of Standards and Technology special publications. In addition, we performed tests of system processes to determine the adequacy and effectiveness of those controls.

In addition, we completed a vulnerability assessment of MCC's general support system and evaluated MCC's process for identifying and correcting/mitigating technical vulnerabilities. This included a review of MCC vulnerability scanning configurations and network vulnerability scan results and comparing them with independent network vulnerability scan results. We also reviewed the status of FISMA audit recommendations for fiscal year 2014 and 2015.[9]

In testing for the adequacy and effectiveness of the security controls, we exercised professional judgment in determining the number of items selected for testing and the method used to select them. We considered relative risk, and the significance or criticality of the specific items in achieving the related control objectives. In addition, we considered the severity of a deficiency related to the control activity and not the percentage of deficient items found compared to the total population available for review. In some cases, this resulted in selecting the entire population. However, in cases that we did not select the entire audit population, the results cannot be projected and if projected may be misleading.

[8] *Audit of the Millennium Challenge Corporation's Fiscal Year 2015 Compliance with the Federal Information Security Management Act of 2002, As Amended* (Audit Report No. A-MCC-16-001-P, October 26, 2015) and *Audit of the Millennium Challenge Corporation's Fiscal Year 2014 Compliance with the Federal Information Security Management Act of 2002* (Audit Report No. A-MCC-14-008-P, September 12, 2014).

[9] Ibid. footnote 9.

MANAGEMENT COMMENTS

MILLENNIUM CHALLENGE CORPORATION
UNITED STATES OF AMERICA

Memorandum

DATE: September 21, 2016

TO: Mr. Mark Norman
Director, Information Technology Audit Division
Office of the Inspector General
Millennium Challenge Corporation

FROM: Mahmoud Bah /s/
Vice President for Administration & Finance and CFO, Acting
Millennium Challenge Corporation

Vincent T. Groh /s/
Chief Information Officer
Department of Administration and Finance
Millennium Challenge Corporation

SUBJECT: MCC's Response to the Draft Report on the *Audit of the Millennium Challenge Corporation's Fiscal Year 2016 Compliance with the Federal Information Security Management Act of 2014, As Amended* Draft Report No. A-MCC-16-XXX-P, dated August 26, 2016

Millennium Challenge Corporation (MCC) appreciates the opportunity to comment on the Fiscal Year 2016 audit of MCC's compliance with the regulatory requirements of the Federal Information Security Management Act of 2014, as amended (FISMA) and considers your role vital in helping to achieve and sustain our FISMA compliance.

Our Management Response to your recommendations follows.

Recommendation 1: We recommend that Millennium Challenge Corporation's Chief Information Officer document and implement a process to update baseline configurations for workstations periodically or document acceptance of the risk.

MCC Management Response: MCC concurs with this recommendation. MCC's Chief Information Officer will document and implement a process to update baseline configurations for workstations that includes periodicity, or accept the risk by September 29, 2017.

Recommendation 2: We recommend that Millennium Challenge Corporation's Chief Information Officer implement written procedures to complete, approve, and maintain users' access request forms for the Contract Management System Audit Tracking and Reporting System in accordance with "MCC Access Control Procedures."

MCC Management Response: MCC concurs with this recommendation. MCC's Chief Information Officer will implement written procedures to complete, approve, and maintain users' access request forms for the Contract Management System Audit Tracking and Reporting System in accordance with "MCC Access Control Procedures" by December 30, 2016.

Recommendation 3: We recommend that Millennium Challenge Corporation's Chief Information Officer either implement environmental controls for the secondary data center and document results or document acceptance of the risk.

MCC Management Response: MCC concurs with this recommendation. MCC's Chief Information Officer will implement environmental controls for the secondary data center and document results or document acceptance of the risk by September 29, 2017.

Recommendation 4: We recommend that Millennium Challenge Corporation's Chief Information Officer document and implement a written physical and environmental protection policy that includes all security controls required by National Institute of Standards and Technology Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," and reflects the current operating environment.

MCC Management Response: MCC concurs with this recommendation. MCC's Chief Information Officer will document and implement a written physical and environmental protection policy that includes all security controls required by National Institute of Standards and Technology Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," and reflects the current operating environment by September 29, 2017.

Recommendation 5: We recommend that Millennium Challenge Corporation's Chief Information Officer document and implement written procedures to manage access to the secondary data center. At a minimum, the procedures should include periodically reviewing logs of personnel entering the data center, and implementing a visitor access log for the data center.

MCC Management Response: MCC concurs with this recommendation. MCC's Chief Information Officer will document and implement a process to written procedures to manage access to the secondary data center, to include periodically reviewing logs of personnel entering the data center, and implementing a visitor access log for the data center by September 29, 2017.

Recommendation 6: We recommend that the Millennium Challenge Corporation's Chief Information Officer activate the alarm in the secondary data center and document the results.

MCC Management Response: MCC concurs with this recommendation. MCC's Chief Information Officer has already activated the alarm in the secondary data center and will document the results by December 30, 2016.

Recommendation 7: We recommend that Millennium Challenge Corporation's Chief Information Officer update the "Configuration Management Policies and Procedures" to include testing and approval requirements by the type of system changes.

MCC Management Response: MCC concurs with this recommendation. MCC's Chief Information Officer will update the "Configuration Management Policies and Procedures" to include testing and approval requirements by the type of system changes by September 29, 2017.

Recommendation 8: We recommend that Millennium Challenge Corporation's Chief Information Officer document and implement policy and procedures that include all personnel security controls required by National Institute of Standards and Technology Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations."

MCC Management Response: MCC concurs with this recommendation. MCC's Chief Information Officer will document and implement a personnel security policy and procedures that addresses all required and applicable personnel security controls as required by National Institute of Standards and Technology Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations" by September 29, 2017.

Recommendation 9: We recommend that the Millennium Challenge Corporation obtain a written, fully executed Interconnection Security Agreement with the Department of Interior's Interior Business Center.

MCC Management Response: MCC concurs with this recommendation. MCC will obtain a written, fully executed Interconnection Security Agreement with the Department of Interior's Interior Business Center by June 30, 2017.

CC: IG/MCC, Alvin Brown
IG/MCC, Lisa Banks
IG/MCC, Fred Jones
IG/MCC, Aleta Johnson
MCC/A&F/FMD, Karla Chryar
MCC/A&F/OCIO, Miguel Adams

Status of Prior Year Findings

The following table provides the status of the FY 2015 FISMA audit recommendations. [10]

No.	FY 2015 Audit Recommendation	MCC Status	Auditor's Position on Status
1	We recommend that the Millennium Challenge Corporation's Chief Information Officer implement automated controls to disable inactive MCCNet accounts when they reach the Corporation's inactivity threshold. If management determines that using such controls are not feasible, document that decision formally and implement mitigating manual controls.	Closed	Agree
2	We recommend that the Millennium Challenge Corporation's Vice President of Administration and Finance document and implement a process to perform periodic, as defined by the Corporation, reviews of the exit clearance process to determine whether personnel are maintaining exit forms as required.	Open	Agree. FY 2016 FISMA Audit noted weaknesses, Please refer to Finding# 8
3	We recommend that the Millennium Challenge Corporation's Chief Information Office develop and implement a written process to validate whether the plans of action and milestones is completed and updated timely.	Closed	Agree
4	We recommend that the Millennium Challenge Corporation's Chief Information Officer document and implement a process to verify whether mobile devices are encrypted prior to use for Corporation business.	Closed	Agree
5	We recommend that the Millennium Challenge Corporation's Chief Information Officer document and implement a process to verify on a periodic basis, as defined by the Corporation, the status of encryption on all mobile devices containing Corporation data and take corrective action, as necessary.	Closed	Agree
6	We recommend that the Millennium Challenge Corporation's Chief Information Officer implement multifactor authentication for all network accounts and document the results.	Open	Agree. FY 2016 FISMA Audit noted weaknesses, Please refer to Finding #9
7	We recommend that the Millennium Challenge Corporation's Chief Information Officer document and implement a written process to ensure system risk assessments are completed in compliance with the Corporation's Risk Assessment Policy and Procedures.	Closed	Agree

[10] *Audit of the Millennium Challenge Corporation's Fiscal Year 2015 Compliance with the Federal Information Security Management Act of 2002, As Amended* (Audit Report No. A-MCC-16-001-P, October 26, 2015).

No.	FY 2015 Audit Recommendation	MCC Status	Auditor's Position on Status
8	We recommend that the Millennium Challenge Corporation's Chief Information Officer complete and implement automated system controls to support the detection and protection of privacy related information.	Closed	Agree

The following table provides the status of the FY 2014 FISMA audit recommendations. [11]

No.	FY 2014 Audit Recommendation	MCC Status	Auditor's Position on Status
1	We recommend that the Millennium Challenge Corporation Chief Information Officer remediate vulnerabilities on the network identified by the Office of Inspector General's contractor, as appropriate, or document acceptance of the risks of those vulnerabilities.	Closed	Agree
4	We recommend that the Millennium Challenge Corporation Chief Information Officer implement and document a process for ensuring contractor systems are continuously monitored and assessed in accordance with the Corporation's policies.	Closed	Agree
5	We recommend that the Millennium Challenge Corporation Chief Information Officer update the Information System Security Policy to address National Institute of Standards and Technology Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.	Closed	Agree

[11] *Audit of the Millennium Challenge Corporation's Fiscal Year 2014 Compliance with the Federal Information Security Management Act of 2002* (Audit Report No. A-MCC-14-008-P, September 12, 2014).

Summary of Results of Each Control Reviewed

(SBU)		
Control	Control Name	Is Control Effective?
MCCNet		
AC-1	Access Control Policy & Procedures	Yes
AC-2	Account Management	Yes
AC-3	Access Enforcement	Yes
AC-4	Information Flow Enforcement	Yes
AC-5	Separation of Duties	Yes
AC-6	Least Privilege	Yes
AC-11	Session Lock	Yes
AC-17	Remote Access	Yes
AC-19	Access Control for Mobile Devices	Yes
AT-1	Security Awareness & Training Policy and Procedures	Yes
AT-2	Security Awareness	Yes
AT-3	Security Training	Yes
AT-4	Security Training Records	Yes
AU-6	Audit, Review, Analysis and Reporting	Yes
CA-1	Security Assessment and Authorization Policy & Procedures	Yes
CA-2	Security Assessments	Yes
CA-3	Information System Connections	No, See finding #7
CA-5	Plan of Action and Milestones	Yes
CA-6	Security Authorization	Yes
CA-7	Continuous Monitoring	Yes
CA-9	Internal System Connections	Yes
CM-1	Configuration Management Policy and Procedures	Yes
[redacted]	[redacted]	[redacted]
CM-3	Configuration Change Control	No, See finding #5
CM-6	Configuration Settings	Yes
CM-7	Least Functionality	Yes
CM-8	Information System Component Inventory	Yes
CM-9	Configuration Management Plan	No, See finding #5
CM-10	Software Usage Restrictions	Yes
CM-11	User-Installed Software	Yes
CP-1	Contingency Planning Policy & Procedures	Yes
CP-2	Contingency Plan	Yes
CP-4	Contingency Plan Testing and Exercises	Yes
CP-6	Alternate Storage Sites	Yes
CP-7	Alternate Processing Sites	Yes

(SBU)		
Control	Control Name	Is Control Effective?
CP-8	Telecommunication Services	Yes
CP-9	Information System Backup	Yes
CP-10	Information System Recovery & Reconstitution	Yes
IA-1	Identification and Authentication Policy and Procedures	Yes
[redacted]	[redacted]	[redacted]
IA-3	Device Identification and Authentication	Yes
IA-5	Authenticator Management	Yes
IR-1	Incident Response Policy and Procedures	Yes
IR-4	Incident Handling	Yes
IR-5	Incident Monitoring	Yes
IR-6	Incident Reporting	Yes
IR-8	Incident Response Plan	Yes
RA-1	Risk Assessment Policy and Procedures	Yes
RA-2	Security Categorization	Yes
RA-3	Risk Assessment	Yes
RA-5	Vulnerability Scanning	Yes
SA-1	System & Services Acquisition Policy and Procedures	Yes
SA-4	Acquisitions Process	Yes
SA-5	Information System Documentation	Yes
SA-9	External Information System Services	Yes
SA-10	Developer Configuration Management	Yes
SA-11	Developer Security Testing and Evaluation	Yes
SC-7	Boundary Protection	Yes
SC-8	Transmission Integrity	Yes
[redacted]	[redacted]	[redacted]
PM-1	Information Security Program Plan	Yes
PM-3	Information Security Resources	Yes
PM-4	Plan of Action and Milestones Process	Yes
PM-5	Information System Inventory	No, See finding #10
PM-6	Information Security Measures of Performance	Yes
PM-7	Enterprise Architecture	Yes
PM-8	Critical Infrastructure Plan	Yes
PM-9	Risk Management Strategy	Yes
PM-10	Security Authorization Process	Yes
[redacted]	[redacted]	[redacted]
PS-2	Position Risk Designation	Yes
PS-3	Personnel Screening	Yes
PS-4	Personnel Termination	No, See finding #8
PS-5	Personnel Transfer	Yes
PS-6	Access Agreements	Yes
PS-7	Third-Party Personnel Security	Yes
PS-8	Personnel Sanctions	Yes
[redacted]	[redacted]	[redacted]

(SBU)		
Control	Control Name	Is Control Effective?
[redacted]	[redacted]	[redacted]
PE-4	Access Control for Transmission Medium	Yes
PE-5	Access Control for Output Devices	Yes
PE-6	Monitoring Physical Access	Yes
[redacted]	[redacted]	[redacted]
PE-9	Power Equipment & Cabling	Yes
[redacted]	[redacted]	[redacted]
PE-11	Emergency Power	Yes
PE-12	Emergency Lighting	Yes
[redacted]	[redacted]	[redacted]
PE-15	Water Damage Protection	Yes
PE-16	Delivery & Removal	Yes
PE-17	Alternate Work Site	Yes
MCC MIS		
AC-2	Account Management	Yes
AC-20	User of External Information Systems	Yes
MCC Public Website		
RA-2	Security Categorization	Yes
AC-20	User of External Information Systems	Yes
MCA Collaborate		
RA-2	Security Categorization	Yes
AC-20	User of External Information Systems	Yes
MCC Contract Management System Audit Tracking and Reporting System		
[redacted]	[redacted]	[redacted]
AC-20	User of External Information Systems	Yes
RA-2	Security Categorization	Yes

U.S. Agency for International Development
Office of Inspector General
1300 Pennsylvania Avenue, NW
Washington, DC 20523
Tel: 202-712-1150
Fax: 202-216-3047
https://oig.usaid.gov
Task Number AM100616