OFFICE OF INSPECTOR GENERAL
Millennium Challenge Corporation

MCC Implemented Controls in Support of FISMA for Fiscal Year 2017 but Improvements Are Needed

AUDIT REPORT A-MCC-17-006-C
SEPTEMBER 28, 2017

1300 Pennsylvania Avenue NW • Washington, DC 20523
oig.usaid.gov • 202-712-1150

The Office of Inspector General provides independent oversight that promotes the efficiency, effectiveness, and integrity of foreign assistance provided through the entities under OIG's jurisdiction: the U.S. Agency for International Development, U.S. African Development Foundation, Inter-American Foundation, Millennium Challenge Corporation, and Overseas Private Investment Corporation.

Report waste, fraud, and abuse

Millennium Challenge Corporation Hotline
Email: mcchotline@usaid.gov
Phone: 202-712-1023 or 800-230-6539
Mail: USAID OIG Hotline, Attn: MCC Hotline, P.O. Box 657, Washington, DC 20044-0657

MEMORANDUM

DATE: September 28, 2017

TO: Chief Information Officer, Vincent Groh

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

SUBJECT: MCC Implemented Controls in Support of FISMA for Fiscal Year 2017, but Improvements Are Needed (A-MCC-17-006-C)

Enclosed is the final audit report on the Millennium Challenge Corporation's (MCC) compliance with the Federal Information Security Modernization Act of 2014 (FISMA) during fiscal year (FY) 2017. The Office of Inspector General (OIG) contracted with the independent certified public accounting firm CliftonLarsonAllen LLP (Clifton) to conduct the audit. The contract required Clifton to perform the audit in accordance with generally accepted government auditing standards.

In carrying out its oversight responsibilities, OIG reviewed Clifton's report and related audit documentation and inquired of its representatives. Our review, which was different from an audit performed in accordance with generally accepted government auditing standards, was not intended to enable us to express, and we do not express, an opinion on MCC's compliance with FISMA. Clifton is responsible for the enclosed auditor's report and the conclusions expressed in it. We found no instances in which Clifton did not comply, in all material respects, with applicable standards.

The audit objective was to determine whether MCC implemented certain 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 the National Institute of Standards and Technology's Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations." Clifton auditors reviewed three of the seven information systems in MCC's inventory as of March 2017. Fieldwork took place at MCC's headquarters in Washington, DC, from March 15 to August 2, 2017.

Clifton concluded that MCC implemented 97 of the 108 selected security controls, which are designed to preserve the confidentiality, integrity, and availability of information and information systems. For example, MCC did the following:

- Implemented an effective incident handling and response program.
- Maintained an effective specialized training program for its employees requiring role-based training.
- Implemented an effective vulnerability identification process.
- Implemented effective whitelisting of software.

However, the auditors found MCC did not fully implement the remaining 11 selected security controls. To address the weaknesses identified, Clifton made and OIG agrees with the following recommendations to MCC's management to address the weaknesses identified; we will track these recommendations until MCC fully implements them. We recommend MCC's chief information officer:

Recommendation 1. Document and implement written procedures for account management that include:

- Completing, approving, and maintaining access request forms.
- Periodically recertifying users' access rights.

Recommendation 2. Document and implement procedures for approving access for global administrator accounts before they are created.

Recommendation 3. Perform a documented review of current procedures to identify any missing 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 should update its documented procedures based on that review to address any missing controls.

Recommendation 4. Document and implement mobile device policies and procedures that address all applicable mobile device controls as required by the MCC Information System Security Policy.

Recommendation 5. Implement written procedures to conduct and maintain security impact analyses before approving requests for changes to system configurations.

In finalizing the report, Clifton evaluated MCC's responses to the recommendations. Both Clifton and OIG acknowledge MCC's management decisions on Recommendations 1 through 5.

We appreciate the assistance extended to our staff and Clifton employees during the engagement.

CliftonLarsonAllen

The Millennium Challenge Corporation has Implemented Many Controls in Support of the Federal Information Security Modernization Act of 2014, But Improvements Are Needed

Fiscal Year 2017

Final Report

CliftonLarsonAllen LLP
901 N. Glebe Road, Suite 200
Arlington, VA 22203

571-227-9500 | fax 571-227-9552

CLAconnect.com

CliftonLarsonAllen

CliftonLarsonAllen LLP
901 N. Glebe Road, Suite 200
Arlington, VA 22203
571-227-9500 | fax 571-227-9552
CLAconnect.com

September 26, 2017

Mr. Mark Norman
Director, Information Technology Audits Division
United States Agency for International Development
Office of the Inspector General
1300 Pennsylvania Avenue, NW
Washington, DC 20005-2221

Dear Mr. Norman:

Enclosed is the final version of our report on the Millennium Challenge Corporation's compliance with the Federal Information Security Modernization Act of 2014 (FISMA), *The Millennium Challenge Corporation Has Implemented Many Controls in Support of FISMA, But Improvements Are Needed*. The USAID Office of Inspector General (OIG) contracted with the independent certified public accounting firm of CliftonLarsonAllen LLP to conduct the 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 certain security controls for selected information systems in support of FISMA. 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.*

For this audit, we reviewed selected controls from MCC's three internal information systems. The audit also included an external vulnerability assessment of MCC's general support system and a wireless assessment. Audit fieldwork was performed at the Millennium Challenge Corporation's headquarters in Washington, D.C., from March 15, 2017, through August 2, 2017.

Our audit was performed in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. 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.

The audit concluded that MCC generally complied with FISMA requirements by implementing many selected security controls for selected information systems. Although MCC generally had policies for its information security program, its implementation of those policies for a subset of 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.

We are making five recommendations to assist MCC in strengthening its information security program. In addition, findings related to seven recommendations from prior years were not yet fully implemented and therefore new recommendations were not made.

This report is for the purpose of concluding on the audit objective described above. Accordingly, this report is not suitable for any other purpose.

We appreciate the assistance we received from the staff of MCC and appreciate the opportunity to serve you. We will be pleased to discuss any questions you may have.

Very truly yours,

CLIFTONLARSONALLEN LLP

CliftonLarsonAllen LLP

TABLE OF CONTENTS

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 to 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 (NIST) are mandatory for Federal agencies.

The United States Agency for International Development's (USAID) Office of Inspector General (OIG) 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 certain minimum 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.

For this audit, we reviewed selected controls from three of MCC's seven information systems[3]. The systems included one general support systems and two major applications.

Results

The audit concluded that MCC generally complied with FISMA requirements by implementing 97 of 108 selected security controls[4] for selected information systems. For example, MCC:

[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 III for a list of controls reviewed.

[3] According to NIST, an information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

[4] ibid. footnote 2.

- Implemented an effective incident handling and response program.

- Maintained an effective specialized training program for its employees requiring role-based training.

- Implemented an effective vulnerability identification process.

- Implemented an effective whitelisting of software.

Although MCC generally had policies for its information security program, its implementation of those policies for 11 of the 108 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 the following areas in MCC's information security program that needed to be improved.

- Account management controls need to be strengthened. (2 controls)

- User access controls need to be implemented. (1 control)

- Policy and procedures to address required information system controls need to be updated (4 controls)

- MCC needs to strengthen configuration management procedures. (1 control)

- MCC needs to fully implement multifactor authentication. (1 control)

- MCC account lockout settings need to be strengthened. (1 control)

- MCC needs to strengthen account inactivity controls. (1 control)

As a result, MCC's operations and assets may be at risk of unauthorized access, misuse and disruption. We made five recommendations to assist MCC in strengthening its information security program. In addition, findings related to seven recommendations from prior years were not yet fully implemented and, therefore, new recommendations were not made.

In response to the draft report, MCC outlined and described its plans to address all five 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.

AUDIT FINDINGS

1. Account Management Controls Need to be Strengthened

NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, security control AC-2, states the following regarding account management:

> The organization:
>
> e. * * *Requires approvals by [*Assignment: organization-defined personnel or roles*] for requests to create information system accounts;
>
> f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [*Assignment: organization-defined procedures or conditions*];
>
> * * *
>
> h. Reviews accounts for compliance with account management requirements [Assig*nment: organization-defined frequency*].

In addition, security control AC-3, states the following regarding access enforcement:

> The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

User access forms were not in place for granting access to 1 of the 3 systems. Specifically, of 20 users, 6 of a sample of 6 users did not have approved access requests forms on file. In addition, there was no process to review and recertify user accounts on a periodic basis.

These account management issues resulted from the lack of detailed user administration (user creation, user approval, user recertification, etc.,) processes.

Without adequate account authorization procedures in place, MCC is at risk of allowing potentially unauthorized access to their systems and data. As a result, we recommend the following:

> ***Recommendation 1:*** *We recommend that the Millennium Challenge Corporation's Chief Information Officer document and implement written procedures for account management to include:*
>
> - *Completing, approving, and maintaining access request forms; and*
> - *Periodically recertifying users' access rights.*

2. User Access Controls Need to be Implemented

NIST Special Publication 800-53, Revision 4, security control AC-2, states the following regarding account management:

> The organization:
>
> e. * * *Requires approvals by [*Assignment: organization-defined personnel or roles*] for requests to create information system accounts;
>
> f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [*Assignment: organization-defined procedures or conditions*].

The MCC system administrator for one of the three sampled systems did not review and approve global administrator account requests before they were created. Due to the system being new, MCC had not developed procedures related to granting access for global administrator accounts. MCC identified this issue during their annual review of controls as part of their continuous monitoring process. MCC created a plan of action and milestone (POA&M) to address the weakness and, at the time of assessment, was working towards remediating the issue.

Without adequate account authorization procedures in place, MCC is at risk of allowing potentially unauthorized access to their systems and data. As a result, we recommend the following:

> ***Recommendation 2:*** *We recommend that the Millennium Challenge Corporation's Chief Information Officer document and implement procedures for approving access for global administrator accounts.*

3. Policy and Procedures to Address Required Information System Controls Need to be Updated

MCC's *Information System Security Policy* (ISSP) states the following regarding system documentation:

> ISSO shall update system documentation annually or whenever significant changes occur.

Additionally, the ISSP goes on to state the following:

> Chief Information Officer (CIO) shall develop access control procedures and review the procedures at least every two years.

MCC did not have comprehensive, documented procedures in place that addresses all required controls as outlined in the following NIST Special Publication 800-53, Revision 4, control families:

- Maintenance
- Audit and Accountability
- Identification and Authentication
- System and Communication Protection

MCC identified these issues during their annual review of controls as part of their continuous monitoring process. POA&Ms were created for each procedure document and MCC began updating the aforementioned procedures. However, at the time of review, MCC had not completed the process of updating the procedures to include all of the required control implementations.

Additionally, *The Use of Personally Owned Devices Policy* has not been reviewed or updated since July 10, 2014. MCC identified this issue during their annual review of controls as part of their continuous monitoring process. MCC created a POA&M to address the weakness and, at the time of assessment, was working towards remediating the issue.

Without documented procedures to reflect current security control standards and environment, MCC may not be adequately implementing the required security controls. In addition, without a current mobile device policy to reflect current standards and environment, MCC may not be adequately implementing the associated mobile device security controls. As a result, we recommend the following:

> ***Recommendation 3:*** *We recommend that the Millennium Challenge Corporation's Chief Information Officer perform a documented review of current procedures to identify any missing 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*. Based on that review, update the documented procedures to address any missing controls.*
>
> ***Recommendation 4:*** *We recommend that the Millennium Challenge Corporation's Chief Information Officer document and implement mobile device policies and procedures that address all applicable mobile device controls as required by the* Millennium Challenge Corporation Information System Security Policy*.*

4. 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:
>
> b. * * *Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses.

Additionally, the *Millennium Challenge Corporation Configuration Management Policy and Procedure* requires System Administrators to:

> Conduct security impact analyses to determine the effects of configuration changes prior to implementation.

Of the 177 closed change requests for fiscal year 2017, 15 of the 15 sampled requests did not have evidence that a security impact analysis was performed as required by policy for one of three systems reviewed. As a process oversight, MCC failed to conduct a security impact analysis to determine the effects of configuration changes prior to implementation. MCC had identified this issue during their annual review of controls as part of their continuous monitoring process and created a POA&M to address the weakness with an anticipated completion date of March 31, 2017. This POA&M was categorized as a low risk POA&M and has been delayed while MCC remediated higher risk POA&Ms. At the time of this report, this POA&M was still open.

Without performing security impact analyses for MCC system configuration changes, MCC is at risk of allowing harmful change requests to be implemented to the production environment. As a result, we recommend the following:

> ***Recommendation 5:*** *We recommend that the Millennium Challenge Corporation's Chief Information Officer implement written procedures to conduct and maintain security impact analyses before approving change requests.*

5. MCC Needs to Fully Implement Multifactor Authentication

According to NIST Special Publication 800-53, Revision 4, security control IA-2, the organization should implement multifactor authentication for network and local access to privileged and non-privileged accounts to gain access to information system.

In addition, Homeland Security Presidential Directive 12: *Policy for a Common Identification Standard for Federal Employees and Contractors* (August 27, 2004) requires the use of Personal Identification Verification (PIV) for gaining logical access to federally controlled information systems.

MCC did not implement multifactor authentication for network access for its non-privileged users. MCC uses the Department of State's (State's) Identity, Credentialing, and Access Management system. However, MCC's card issuing system previously could not issue contractors their certificates until the system was upgraded. Delays for the system upgrade extended over a year while the State Department completed an authorization to operate for the upgraded system. The State Department completed the authorization to operate on October 4, 2016, which now allows MCC to issue certificates to all MCC employees. MCC has implemented multi-factor authentication for privileged users, but at the time of assessment implementation had not completed for all non-privileged users. MCC plans to complete implementation of multi-factor authentication for all users by the end of fiscal year 2017.

By not implementing multifactor authentication for access to MCC's network, 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;[5] however, procedures were not fully implemented and MCC had not closed the recommendation. Therefore, we are not making additional recommendations at this time.

[5] 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).

6. MCC Account Lockout Settings Need to be Strengthened

NIST Special Publication 800-53, Revision 4, security control AC-11, states the following regarding session lock:

> The information system:
>
> a. Prevents further access to the system by initiating a session lock after [*Assignment: organization-defined time period*] of inactivity or upon receiving a request from a user; and
>
> b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

In addition, MCC's *System Security Plan*, dated March 2017, required accounts to be automatically locked for a defined time-period after a certain number of consecutive failed logon attempts.

However, the current security parameters for 1 of the 3 systems reviewed were set to a weaker setting than what was specified by MCC's *System Security Plan*. This occurred as an oversight as management had not updated the configuration settings to reflect the ISSP policy.

Without strong account lockout controls there is an increased risk of an unauthorized user gaining access to the system. Upon notification of the issue, MCC updated their configuration settings to correct this weakness. Therefore, we are not making a recommendation at this time.

7. MCC Needs to Strengthen Account Inactivity Controls

NIST Special Publication 800-53, Revision 4, security control AC-2, states the following regarding account management:

> The organization:
>
> * * *
>
> f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [*Assignment: organization-defined procedures or conditions*];

For one of three systems, MCC's Access Control Plan had a discrepancy in the amount of time that a user account can be inactive before the system automatically disables the account. This occurred because of a management oversight in developing the Access Control Plan.

Without consistent security policy and control implementations, security deficiencies and vulnerabilities may exist that go undetected. Upon notification of the issue, MCC updated the Access Control Plan. 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 five 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 five recommendations.

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 certain security controls for selected information systems[6] in support of the Federal Information Security Modernization Act of 2014 (FISMA).

The audit included tests 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
- Maintenance
- Personnel Security
- 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 three of the seven systems in MCC's inventory as of March 2017. See Appendix III for a listing of selected controls for each system. The audit also included an external vulnerability assessment of MCC's general support system and a

[6] See Appendix III for a list of controls selected.

wireless vulnerability assessment. The audit also included a follow up on prior audit recommendations[7] 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 15, 2017, to August 2, 2017.

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 an external vulnerability assessment of one of MCC's systems 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. In addition, a wireless assessment was conducted on-site. We also reviewed the status of FISMA audit recommendations for fiscal years 2015 and 2016.[8]

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.

[7] *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) and *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).

[8] Ibid. footnote 6.

Management Comments

MILLENNIUM
CHALLENGE CORPORATION
UNITED STATES OF AMERICA

Memorandum

DATE: September 8, 2017

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

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

Vincent T. Groh
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 2017 Compliance with the Federal Information Security Management Act of 2014, As Amended* Draft Report No. A-MCC17-00X-C, dated August 31, 2017

Millennium Challenge Corporation (MCC) appreciates the opportunity to comment on the Fiscal Year 2017 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 the Millennium Challenge Corporation's Chief Information Officer document and implement written procedures for account management to include:

- Completing, approving, and maintaining access request forms; and
- Periodically recertifying users' access rights.

MCC Management Response: MCC concurs with this recommendation. MCC's Chief Information Officer will document and implement account management procedures that include: a) completing, approving, and maintaining access request forms; and b) periodic recertification of user's access rights by January 30, 2018.

Recommendation 2. We recommend that the Millennium Challenge Corporation's Chief Information Officer document and implement procedures for approving access for global administrator accounts.

MCC Management Response: MCC concurs with this recommendation and will document and implement a process that requires approval before the creation of all global administrator accounts by December 15, 2017.

Recommendation 3. We recommend that the Millennium Challenge Corporation's Chief Information Officer perform a documented review of current procedures to identify any missing 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. Based on that review, update the documented procedures to address any missing controls.

MCC Management Response: MCC concurs with this recommendation and will perform and document an a review of all current procedures to ensure they align with National Institute of Standards and Technology Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, and update the documented procedures to address any missing controls by August 30, 2018.

Recommendation 4. We recommend that the Millennium Challenge Corporation's Chief Information Officer document and implement mobile device policies and procedures that address all applicable mobile device controls as required by the MCC Information System Security Policy.

MCC Management Response: MCC concurs with this recommendation and will document and implement a mobile device policy and procedures by April 30, 2018.

Recommendation 5. We recommend that the Millennium Challenge Corporation's Chief Information Officer implement written procedures to conduct and maintain security impact analyses before approving change requests.

MCC Management Response: MCC concurs with this recommendation and will document and implement procedures for conducting a security impact analysis during the change management process by December 15, 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

Summary of Controls Reviewed

Control	Control Name	Number of Systems Tested
AC-1	Access Control Policy & Procedures	1
AC-2	Account Management	3
AC-3	Access Enforcement	1
AC-4	Information Flow Enforcement	1
AC-5	Separation of Duties	3
AC-6	Least Privilege	3
AC-11	Session Lock	1
AC-17	Remote Access	1
AC-19	Access Control for Mobile Devices	1
AC-20	Use of External Information Systems	3
AT-1	Security Awareness & Training Policy and Procedures	1
AT-2	Security Awareness	1
AT-3	Role-Based Security Training	1
AT-4	Security Training Records	1
AU-1	Audit & Accountability Policy and Procedures	1
AU-2	Auditable Events	1
AU-3	Content of Audit Records	1
AU-4	Audit Storage Capacity	1
AU-5	Response to Audit Processing Failures	1
AU-6	Audit, Review, Analysis and Reporting	1
AU-7	Audit Reduction & Report Generation	1
AU-8	Time Stamps	1
AU-9	Protection of Audit Information	1
AU-10	Non-repudiation	1
AU-11	Audit Record Retention	1
AU-12	Audit Generation	1
CA-1	Security Assessment and Authorization Policy & Procedures	1
CA-2	Security Assessments	1
CA-3	System Interconnections	1
CA-5	Plan of Action and Milestones	1
CA-6	Security Authorization	1
CA-7	Continuous Monitoring	1
CA-8	Penetration Testing	1
CA-9	Internal System Connections	1
CM-1	Configuration Management Policy & Procedures	1
CM-2	Baseline Configuration	1
CM-3	Configuration Change Control	1
CM-6	Configuration Settings	1
CM-7	Least functionality	1
CM-8	Information System Component Inventory	1
CP-1	Contingency Planning Policy & Procedures	1
CP-2	Contingency Plan	1

Control	Control Name	Number of Systems Tested
CP-4	Contingency Plan Testing and Exercises	1
CP-6	Alternate Storage Sites	1
CP-7	Alternate Processing Sites	1
CP-8	Telecommunication Services	1
CP-9	Information System Backup	1
CP-10	Information System Recovery & Reconstitution	1
IA-1	Identification & Authentication Policy and Procedures	1
IA-2	Identification & Authentication (Organizational Users)	1
IA-3	Device Identification & Authentication	1
IA-4	Identifier Management	1
IA-5	Authenticator Management	1
IR-1	Incident Response Policy & Procedures	1
IR-4	Incident Handling	1
IR-5	Incident Monitoring	1
IR-6	Incident Reporting	1
IR-8	Incident Response Plan	1
MA-1	System Maintenance Policy and Procedures	1
MA-2	Controlled Maintenance	1
MA-3	Maintenance Tools	1
MA-4	Nonlocal Maintenance	1
MA-5	Maintenance Personnel	1
MA-6	Timely Maintenance	1
PM-1	Information Security Program Plan	1
PM-3	Information Security Resources	1
PM-4	Plan of Action and Milestones Process	1
PM-5	Information System Inventory	1
PM-6	Information Security Measures of Performance	1
PM-7	Enterprise Architecture	1
PM-8	Critical Infrastructure Plan	1
PM-9	Risk Management Strategy	1
PM-10	Security Authorization Process	1
PS-6	Access Agreements	1
RA-1	Risk Assessment Policy and Procedures	1
RA-2	Security Categorization	3
RA-3	Risk Assessment	3
RA-5	Vulnerability Scanning	1
SA-1	System & Services Acquisition Policy and Procedures	1
SA-4	Acquisitions Process	1
SA-5	Information System Documentation	1
SA-9	External Information System Services	1
SA-10	Developer Configuration Management	1
SA-11	Developer Security Testing and Evaluation	1
SC-1	System & Communications Protection Policy & Procedures	1
SC-10	Network Disconnect	1
SC-12	Cryptographic Key Establishment & Management	1

Control	Control Name	Number of Systems Tested
SC-13	Use of Cryptography	1
SC-14	Public Access Protections	1
SC-15	Collaborative Computing	1
SC-17	Public Key Infrastructure Certificates	1
SC-2	Application Partitioning	1
SC-5	Denial of Service Protection	1
SC-7	Boundary Protection	1
SC-8	Transmission Integrity	1
SI-2	Flaw remediation	1