OFFICE OF INSPECTOR GENERAL

AUDIT OF THE MILLENNIUM CHALLENGE CORPORATION'S FISCAL YEAR 2012 COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002

AUDIT REPORT NO. M-000-13-001-P
NOVEMBER 6, 2012

WASHINGTON, D.C.

Office of Inspector General

November 6, 2012

Ms. Chantale Y. Wong
Vice President of Administration and Finance
Millennium Challenge Corporation
875 Fifteenth Street, N.W.
Washington, DC 20005

Subject: Audit of the Millennium Challenge Corporation's Fiscal Year 2012 Compliance With the Federal Information Security Management Act of 2002 (Report No. M-000-13-001-P).

Dear Ms. Wong:

Enclosed is the final report on the "Audit of the Millennium Challenge Corporation's Fiscal Year 2012 Compliance With the Federal Information Security Management Act of 2002" (Report No. M-000-13-001-P). The Office of Inspector General (OIG) contracted with the independent certified public accounting firm of CliftonLarsonAllen LLP (Clifton) to conduct the audit. Clifton was required to conduct the audit in accordance with U.S. generally accepted government auditing standards. Appendix I of Clifton's report describes the scope and methodology used for the audit.

The audit found that MCC implemented 86 of 103 selected security controls for selected information systems in support of the Federal Information Security Management Act. For example, Clifton found that MCC complied with the requirements to:

- Categorize the information systems and the information processed, stored, or transmitted in accordance with federal guidelines.

- Implement an effective incident handling and response program.
- Establish an effective media protection program.
- Maintain an adequate and effective specialized training program for its employees.
- Implement an effective identification and authentication program.
- Establish appropriate segregation of duties in MCCNet, MCC's general support system.

However, Clifton identified aspects of MCC's information security program that can be improved. Specifically, MCC needs to:

- Strengthen security controls for patch and configuration management.
- Periodically review network accounts.
- Strengthen personnel out-processing procedures.
- Assess system risks and maintain current system Authorizations to Operate.
- Conduct system security assessments as specified by the National Institute of Standards and Technology.
- Ensure all personnel receive security awareness training.
- Implement effective asset management controls.
- Document configuration management procedures.
- Periodically test contingency plans.
- Assess and update security policies.
- Update the MCCNet System Security Plan.
- Strengthen risk management controls.

Consequently, MCC's operations and assets may be at risk of misuse and disruption. Clifton's report makes 18 recommendations to assist MCC in strengthening its information security program.

In connection with our contract, we reviewed Clifton's report and related audit documentation. Our review was different from an audit conducted 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 MCC's compliance with the Federal Information Security Management Act of 2002. Clifton is responsible for the enclosed auditor's report and the conclusions

expressed in the report. Our review disclosed no instances in which Clifton did not comply, in all material respects, with applicable standards.

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

Recommendation 1. *We recommend that the Millennium Challenge Corporation Chief Information Officer establish written time frames for implementing patches to ensure the remediation of known vulnerabilities.*

Recommendation 2. *We recommend that the Millennium Challenge Corporation Chief Information Officer review the critical and high-risk vulnerabilities identified by the Office of Inspector General contractor and document why the Corporation's vulnerability management tool is not identifying these vulnerabilities.*

Recommendation 3. *We recommend that the Millennium Challenge Corporation Chief Information Officer document and implement a process for documenting management review, acceptance, and implementation of corresponding compensating controls for known vulnerability scan exclusions.*

Recommendation 4. *We recommend that the Millennium Challenge Corporation Chief Information Officer document and implement a process to conduct periodic reviews, as defined by the Corporation, of MCCNet users' access privileges to verify that they are appropriate.*

Recommendation 5. *We recommend that the Millennium Challenge Corporation Chief Information Officer document and implement a process to review active accounts whose owners have never logged into the system to determine whether the accounts are necessary.*

Recommendation 6. *We recommend that the Millennium Challenge Corporation 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 ensure its regular implementation.*

Recommendation 7. *We recommend that the Millennium Challenge Corporation Chief Information Officer conduct a full system reauthorization for MCCNet in accordance with the Corporation's policy.*

Recommendation 8. *We recommend that the Millennium Challenge Corporation Chief Information Officer implement a documented validation process to ensure that security impact assessments are conducted prior to significant system changes in accordance with the Corporation's policy.*

Recommendation 9. *We recommend that the Millennium Challenge Corporation Chief Information Officer implement a documented validation process to ensure that system risk assessments are reviewed and updated annually, as required by the* Information Systems Security Policy.

Recommendation 10. *We recommend that the Millennium Challenge Corporation Chief Information Officer document and implement a continuous monitoring plan to assess an appropriate number of controls for the Corporation's information systems periodically, as defined by the Corporation.*

Recommendation 11. *We recommend that the Millennium Challenge Corporation Chief Information Security Officer document and implement metrics for accepting Tips of the Day participation as annual security awareness training.*

Recommendation 12. *We recommend that the Millennium Challenge Corporation Chief Information Security Officer document and implement a process to track and validate that all employees and contractors receive annual security awareness training either by responding to the Tips of the Day or by taking another acceptable security awareness training.*

Recommendation 13. *We recommend that the Millennium Challenge Corporation Chief Information Officer document and implement asset management procedures to include processes for ensuring information system assets are tracked appropriately and that inventories are performed periodically, as defined by the Corporation.*

Recommendation 14. *We recommend that the Millennium Challenge Corporation Chief Information Officer re-open Recommendation 9 in Office of Inspector General Audit Report No. M-000-10-004-P.*

Recommendation 15. *We recommend that Millennium Challenge Corporation Chief Information Officer implement a documented validation process to ensure the annual testing of contingency plans and timely reporting of lessons learned, as required by the* Information System Security Policy*.*

Recommendation 16. *We recommend that the Millennium Challenge Corporation Chief Information Officer re-open Recommendation 9 in Office of Inspector General Audit Report No. M-000-11-004-P.*

Recommendation 17. *We recommend that the Millennium Challenge Corporation Chief Information Officer re-open Recommendation 10 in Office of Inspector General Audit Report No. M-000-11-004-P.*

Recommendation 18. *We recommend that the Millennium Challenge Corporation Chief Information Officer re-open Recommendation 13 in Office of Inspector General Audit Report No.* M-000-11-001-O*.*

In finalizing the report, Clifton evaluated MCC's response to the draft audit report and the recommendations contained therein. Clifton determined that MCC agreed to take appropriate corrective actions for each of the recommendations. Thus, Clifton agreed with MCC's management decisions for Recommendations 1 through 18.

OIG agrees with Clifton's evaluation of MCC's management decisions and, thus, agrees with MCC's management decisions for Recommendations 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, and 18.

OIG appreciates the cooperation and courtesies extended to our staff and to the staff of CliftonLarsonAllen LLP.

Sincerely,

/s/

Richard J. Taylor
Deputy Assistant Inspector General for Audit
Millennium Challenge Corporation

cc:
Paul S. Malone, Chief Information Officer
Terry Bowie, Chief Financial Advisor
Arlene McDonald, Compliance Officer

Audit of the Millennium Challenge Corporation's Compliance with the Federal Information Security Management Act of 2002

Fiscal Year 2012

Final Report
Sensitive But Unclassified

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

www.cliftoncpa.com

TABLE OF CONTENTS

SUMMARY OF RESULTS

The Federal Information Security Management Act of 2002[1] (FISMA) requires agencies to develop, document, and implement an agencywide 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 audit was performed in support of the FISMA requirement for an annual evaluation of MCC's information security program. The objective of this audit was to determine whether MCC implemented selected minimum security controls for selected information systems[2] to meet the Federal Information Security Management Act of 2002 to reduce the risk of data tampering, unauthorized access to and disclosure of sensitive information, and disruption to MCC's operations.

At the time of the audit, MCC's system inventory included one internal system, MCCNet general support system; one internal major application, MCC Integrated Data Analysis System (MIDAS); and seven third-party major applications: (1) National Business Center Oracle Federal Financials, (2) National Business Center Federal Personnel and Payroll System, (3) e-Official Personnel Folder, (4) e-Travel, (5) MCC Public Website, (6) International Treasury Services, and (7) MCC Contract Management System.

The audit concluded that MCC implemented 86 of 103 selected security controls[3] for selected information systems in support of the Federal Information Security Management Act. For example, MCC complied with the following requirements:

- Categorizing the information systems and the information processed, stored or transmitted in accordance with Federal guidelines and designating senior-level officials within the organization to review and approve the security categorizations.

- Implementing an effective incident handling and response program.

[1] Enacted as Title III of the E-Government Act of 2002, Public Law 107-347 (2002). Section 301 of the Act added a new subchapter on information security to the United States Code at 44 U.S.C 3541-3549.
[2] See Appendix IV for a list of controls selected.
[3] See Appendix IV – Summary of Results of Each Control Reviewed.

- Establishing an effective media protection program.
- Maintaining an adequate and effective specialized training program for its employees.
- Implementing an effective identification and authentication program.
- Establishing appropriate segregation of duties within MCCNet.

However, the audit identified areas in MCC's information security program that can be improved. Specifically, MCC needs to:

- Strengthen security controls surrounding patch and configuration management.
- Periodically review network accounts.
- Strengthen personnel out-processing procedures.
- Assess system risks and maintain current system Authorizations to Operate.
- Conduct system security assessments as specified by NIST.
- Ensure all personnel receive security awareness training.
- Implement effective asset management controls.
- Document configuration management procedures.
- Periodically test contingency plans.
- Assess and update security policies.
- Update the MCCNet System Security Plan.
- Strengthen risk management controls.

Consequently, MCC's operations and assets may be at risk of misuse and disruption. This report makes 18 recommendations to assist MCC in strengthening its information security program (pages 3 -15).

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

In response to the draft report, MCC agreed with the audit findings and the recommendations made in the report. MCC outlined its plans to address all 18 audit recommendations and described planned actions to address the recommendations. We agree with MCC's planned actions on all 18 audit recommendations (page 16). MCC's comments are included in their entirety in Appendix II (pages 19-23).

AUDIT FINDINGS

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

MCC had procedures in place that use vulnerability scanning software, nCircle,[4] to assist in detecting and reporting security vulnerabilities. However, using the software tool Nessus, 17 additional vulnerabilities from a sample of 45 critical and high vulnerabilities were identified on MCC hosts that MCC did not identify through its scans. For example, the following patch management related vulnerabilities were not identified by nCircle: ActiveX Kill bits, Citrix ICA Client, PHP, Flash Player, Adobe AIR and DirectX.

Additionally, Common Vulnerabilities Exposures (CVE), a public dictionary of known vulnerabilities, numbers showed that 21 of the sample of vulnerabilities were publicly known before December 2011 including patch vulnerabilities relating to Java, Adobe Shockwave, Microsoft IIS, Cryptographic API Component Object Model, and Microsoft Foundation Class (MFC) library. Several of these vulnerabilities had been known since 1999 and 2000 including a SunSSH patch vulnerability.

The use of different vulnerability scanning tools, patch management timelines, significance of patches, and assignment of risk will affect the vulnerabilities identified by scanning tools. MCC had remediated vulnerabilities on the majority of hosts with the application of patches on nCircle reports. However, subsequent nCircle reports published an overall lower risk score drawing remediation attention away from the few hosts that had not been patched. MCC patch management procedures focus on addressing the host risk score and not the vulnerability. This resulted in a small number of vulnerable hosts perpetuating risk for extended periods of time. Often these older patches have a higher vulnerability rating through the Nessus tool or are not reported in the nCircle scans.

MCC also had not patched specific workstations due to business application requirements; however, the Corporation had not formally documented management's risk acceptance of not patching due to business requirements or vulnerabilities that were excluded from scans and patching.

National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, security control SI-3, states the following regarding malicious code protection:

> The organization:
>
> a. Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code:
>
> - Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or

[4] MCC uses nCircle's IP360 application for vulnerability management.

- Inserted through the exploitation of information system vulnerabilities;

b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures.

Additionally, security control RA-5, states the agency is responsible for the following:

> The organization:
> * * *
> d. Remediates legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk.

NIST Special Publication 800-40, Revision 2, *Creating a Patch and Vulnerability Management Program,* states the following regarding deploying vulnerability remediations: "Organizations should deploy vulnerability remediations to all systems that have the vulnerability, even for systems that are not at immediate risk of exploitation."

Unmitigated vulnerabilities on the MCC network can compromise the confidentiality, integrity, and availability of information on the network. For example:

- An attacker may leverage known issues to execute arbitrary code.
- Agency employees may be unable to access systems.
- Agency data may be compromised.

As a result of the identified vulnerabilities, we are making the following recommendations:

Recommendation 1: *We recommend that the Millennium Challenge Corporation Chief Information Officer establish patch timeframe requirements to ensure remediation of known vulnerabilities.*

Recommendation 2: *We recommend that the Millennium Challenge Corporation Chief Information Officer review the critical and high risk vulnerabilities identified by the Office of Inspector General contractor and document why the vulnerabilities are not being identified by the Corporation's vulnerability management tool.*

Recommendation 3: *We recommend that the Millennium Challenge Corporation Chief Information Officer document and implement a process for documenting management review, acceptance and corresponding compensating controls for known vulnerability scan exclusions.*

2. MCC Needs to Periodically Review Network Accounts

MCC did not perform quarterly reviews of MCCNet group memberships as documented within the *MCC Access Control Procedures*. Management had not implemented a process to periodically review account privileges as they were unaware that such reviews needed to be performed in addition to the weekly review for inactive accounts.

In addition, five user accounts had never been logged into and remained active on the network for more than 30 days. According to Chief Information Security Office

contractor staff, management was performing reviews to identify inactive accounts as well as those that had never logged onto the network; however, many of the accounts belonged to new hires that had yet to log in. Rationale for why new hires were not logging into the network near their start dates was not known. The Chief Information Security Office personnel ran scripts to identify accounts that had not logged in for over 30 days and those that had never logged in. However, the helpdesk did not disable accounts that had never logged in because it could cause confusion or problems for new hires; therefore, the scripts were adjusted to notify the helpdesk only of accounts that had been inactive for more than 30 days.

Section 2.1.1.10, Auditing Group Membership, of the *MCC Access Control Procedures*, states, "MCC uses a limited number of groups to grant permissions to data throughout the agency. Primarily, these sensitive groups include the Office of Human Resources and the Contracts Division (MCC Contracts Division). These groups will be audited at least on a quarterly basis. This auditing will consist of verification of group membership by an assigned owner of the group, being someone of supervisory status within the division."

In addition, NIST Special Publication 800-53, Revision 3, security control AC-2, states the following regarding account management:

> The organization manages information system accounts, including:
>
> * * *
>
> c. Identifying authorized users of the information system and specifying access privileges;
>
> * * *
>
> e. Establishing, activating, modifying, disabling, and removing accounts;
>
> * * *
>
> g. Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;
>
> h. Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users;
>
> * * *
>
> j. Reviewing accounts [*Assignment: organization-defined frequency*].

By not performing periodic reviews/recertification of user accounts, there is an increased risk of unauthorized access to critical systems or incompatible functions being performed. Not disabling inactive or unnecessary accounts also increases the risk of unauthorized access to the system. In addition, failing to deactivate dormant accounts exposes the system to intruders who can leverage the accounts to commit fraud or to obtain sensitive information. As a result, we recommend the following:

> ***Recommendation 4:*** *We recommend that the Millennium Challenge Corporation Chief Information Officer document and implement a process to conduct periodic reviews, as defined by the Corporation, of MCCNet users to verify that appropriate access privileges have been assigned.*

Recommendation 5: *We recommend that the Millennium Challenge Corporation Chief Information Officer document and implement a process to review active accounts that have never logged into the system to determine whether accounts are necessary.*

3. MCC Needs to Strengthen Personnel Out-Processing Procedures

MCC personnel exit checklists were not maintained in the Staff Track and Reconciliation System (STARS) as noted in the *MCC Exit Policy and Clearance Procedures*. The procedures were approved on April 27, 2012; therefore, two quarters of the fiscal year were not covered by the policy. Additionally, while the new exit process had been announced and the technology implemented, the process had not been adopted by the stakeholders involved: Human Resources, Contracts, and Office of Security.

MCC Exit Policy and Clearance Procedures, Section 6.0, Policy, states, "All individuals of the MCC workforce must officially exit the agency by initiating a planned separation and completing the appropriate MCC Exit Form based on their workforce category. In the event that circumstances will not enable an individual of the MCC workforce to initiate separation prior to two weeks from their anticipated departure date, he/she must complete the process for a short notice/unplanned separation." Section 6.1 details that in the event of a planned separation, the MCC Exit Form is to be initiated by the employee (federal employees) or the project monitor/contracting officer's representative (contractors). Upon completion of all exit appointments and the return of all MCC property/equipment, representatives must access the individual's pending Exit Form and provide a digital signature. The completed form will be retained in SharePoint and the individual's STAR record will annotate that the exit process has been completed.

NIST Special Publication 800-53, Revision 3, security control PS-4, states the following regarding personnel termination:

> The organization, upon termination of individual employment:
>
> a. Terminates information system access;
> b. Conducts exit interviews;
> c. Retrieves all security-related organizational information system-related property; and,
> d. Retains access to organizational information and information systems formerly controlled by terminated individual.

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. As a result, we recommend the following:

Recommendation 6: *We recommend that the Millennium Challenge Corporation 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 ensure its implementation.*

4. MCC Needs to Maintain Current System Authorizations to Operate and Assess System Risks

MCC did not properly assess system risks on MCCNet and MIDAS for the fiscal year. For example:

- MCC had not maintained a current Authorization to Operate (ATO) for the MCCNet General Support System. The ATO expired on June 8, 2012, without MCC completing a reauthorization of the system.
- MCC had not performed a security impact assessment prior to moving its data center from Newark, Delaware to Culpeper, Virginia.
- MCC had not completed a risk assessment to reflect the new Culpeper, Virginia data center. The last revision to the risk assessment was dated June 8, 2009.

Management delayed the MCCNet security reauthorization until completion of the data center move. It was indicated that a risk assessment was to be performed with the reauthorization of the system. The MCCNet reauthorization is expected to be completed during the 2013 calendar year.

In addition, a current risk assessment for the MIDAS system had not been completed on an annual basis. Specifically, the last risk assessment was documented in 2010. This occurred because MCC had previously included the MIDAS system risk assessment as part of the system security plan; however, the risk assessment was not revised annually with the security plan to reflect current risks.

MCC's Information Systems Security Policy, Section 9.1 Certification and Accreditation and Risk Assessment states: "System Owners must do the following for the systems they own in support of the MCC Certification and Accreditation (C&A) program: Conduct a new C&A every three years or whenever there is a major change to the system. System owners must conduct an annual security assessment that includes a risk assessment, system security plan, and a revised POA&M."

NIST Special Publication 800-53, Revision 3, security control CA-6, states the following regarding security authorizations:

> The organization:
> * * *
> b. Ensure that the authorizing official authorizes the information system for processing before commencing operations; and,
> c. Updates the security authorization [*Assignment: organization-defined frequency].*

In addition, security control RA-3, states the following regarding risk assessments:

> The organization:
> * * *
> c. Reviews risk assessment results [*Assignment: organization-defined frequency*]; and,

d. Updates the risk assessment [*Assignment: organization-defined frequency*] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

Without completing the security reauthorization process, senior level agency officials may not have taken the appropriate steps to mitigate or accept risks to their information systems. In addition, without current system risk assessments, it is difficult to determine the probability of occurrence, the resulting impact, and the additional safeguards needed to mitigate the impact of potential risks to the systems environment. As a result, we recommend the following:

Recommendation 7: *We recommend that the Millennium Challenge Corporation Chief Information Officer conduct a full system reauthorization for MCCNet in accordance with Corporation's policy.*

Recommendation 8: *We recommend that the Millennium Challenge Corporation Chief Information Officer implement a documented validation process to ensure security impact assessments are conducted prior to significant system changes in accordance with the Corporation's policy.*

Recommendation 9: *We recommend that the Millennium Challenge Corporation Chief Information Officer implement a documented validation process to ensure system risk assessments are reviewed and updated on an annual basis, as required by the* Information System Security Policy*.*

5. MCC Needs to Conduct System Security Assessments as Specified by NIST

The fiscal year 2012 security assessment for MCCNet only covered two control families from NIST Special Publication 800-53, Revision 3: Access Controls and Media Protection. However, this was not in accordance with the NIST Special Publication 800-37, Revision 1, risk management framework and continuous monitoring. The risk management framework and continuous monitoring require the information system owner to identify the security controls to be monitored, the frequency of monitoring, and the control assessment approach.

MCC's current annual system assessment review process does not define a minimum number of controls or control families to be tested. MCC does perform monthly vulnerability scans and daily network monitoring; however, this does not encompass a significant number of management and operational controls. In addition, MCC had not implemented a continuous monitoring process as noted by NIST Special Publication 800-37, Revision 1. Currently, MCC policy states system assessments are only required to include a subset of controls or control families.

NIST Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems* states, "Organizations assess all security controls employed within and inherited by the information system during the initial security authorization. Subsequent to the initial authorization, the organization assesses

a subset of the security controls (including management, operational, and technical controls) on an ongoing basis during continuous monitoring. The selection of appropriate security controls to monitor and the frequency of monitoring are based on the monitoring strategy developed by the information system owner or common control provider and approved by the authorizing official and senior information security officer."

Without testing a rotation of controls periodically, MCC is not able to confirm controls are functioning effectively and may expose the agency to information loss, fraud or abuse. As a result, we recommend the following:

> ***Recommendation 10:*** *We recommend that the Millennium Challenge Corporation Chief Information Officer document and implement a continuous monitoring plan to assess an appropriate number of controls for the organization's information systems on a Corporation-defined frequency.*

6. MCC Needs to Ensure All Personnel Receive Security Awareness Training

MCC did not ensure all personnel were receiving security awareness training. For example, 1 from a sample of 15 individuals had not participated in security awareness training through the Tips of the Day.

MCC was not tracking users who failed to participate in the daily Tips of the Day. In addition, MCC did not establish a required number of tips a user must view each month or year. Additionally, the user who had not participated in training was an overseas employee who accesses the MCC network on a limited basis. MCC Chief Information Security Office contractor staff indicated that there was a possibility that the execution of the login script that runs the Tips of the Day process may function inconsistently for VPN users.

MCC Information Systems Security Policy states as part of Section 3, Roles and Responsibilities, "c. The Chief Information Security Officer (CISO) Designated by the MCC Chief Information Officer is directly responsible for overseeing and executing MCC's information systems security program and has the following responsibilities: (…) Ensuring that agency personnel, including contractors, receive appropriate information security awareness training."

NIST Special Publication 800-53, Revision 3, security control AT-2, states the following regarding security awareness: The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and [*Assignment: organization-defined frequency*] thereafter.

Without the proper IT security awareness training, MCC employees may inadvertently violate security policies and compromise MCC's security. As a result, we recommend the following:

> ***Recommendation 11:*** *We recommend that the Millennium Challenge Corporation Chief Information Security Officer document and implement metrics for accepting Tip of the Day participation as annual security awareness training.*

Recommendation 12: *We recommend that the Millennium Challenge Corporation Chief Information Security Officer document and implement a process to track and validate that all employees and contractors receive the annual security awareness training through either the Tips of the Day program or by taking another acceptable security awareness training.*

7. MCC Needs to Implement Effective Asset Management Controls

MCC did not effectively track and maintain their asset inventory. For example, 4 out of a sample of 11 assets were not located during a walkthrough:

- An asset was noted as being in the MCC inventory; however, it was determined that the asset was owned by a telecommunications service provider. The provider had since transferred the asset offsite; however, the asset inventory database did not reflect this information.
- A laptop was loaned out; however, asset management personnel could not locate this device.
- A server that did not have a location identified in the asset inventory database.
- A desktop could not be located within the defined location as noted in the asset inventory database; however, the desktop was located after the walkthrough.

Asset management personnel did not follow a set of documented procedures for how to manage the asset inventory. In addition, MCC did not conduct periodic wall-to-wall asset inventories. The assets were counted in inventory if asset management personnel were aware of an asset's relocation; however, relocation was not consistently noted in the asset inventory. Additionally, asset management personnel did not have access to offsite locations where additional MCC assets were stored.

NIST Special Publication 800-53, Revision 3, security control CM-8, states the following regarding information system component inventory:

> The organization develops, documents, and maintains an inventory of information system components that:
>
> a. Accurately reflects the current information system;
> b. Is consistent with the authorization boundary of the information system;
> c. Is at the level of granularity deemed necessary for tracking and reporting;
> d. Includes [*Assignment: organization-defined information deemed necessary to achieve effective property accountability*]; and
> e. Is available for review and audit by designated organizational officials.
>
> Control Enhancements:
>
> 1) The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.
>
> * * *
>
> 5) The organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.

Without proper tracking of inventory, MCC did not have an accurate account of which computer assets the Corporation needed to protect. As a result, we recommend the following:

Recommendation 13: *We recommend that the Millennium Challenge Corporation Chief Information Officer document and implement asset management procedures to include processes for ensuring information system assets are tracked appropriately, and that periodic, as defined by the Corporation, information system asset inventories are performed.*

8. MCC Needs to Document Configuration Management Procedures

For a sample of 25 MCCNet change requests, we noted the following:

- 20 did not have test results documented.
- 14 did not have test plans documented.
- 8 did not have a requestor noted.

As a result of the fiscal year 2010 FISMA audit, a recommendation[5] was made for MCC to document, disseminate and implement configuration management procedures. Based on our review this year, MCC closed the recommendation with the updated System Development Lifecycle (SDLC) Guide; however, procedures documenting the types of changes and levels of testing applied to changes were not documented in the SDLC Guide. Therefore, MCC did not have documented change management procedures that describe types of changes and levels of testing applied to the changes prior to approval by the Configuration Control Board.

NIST Special Publication 800-53, Revision 3, security control CM-1, states the following regarding configuration management policies and procedures:

> The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:
>
> a. A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
> b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

NIST Special Publication 800-53, Revision 3, states as part of security control CM-3, configuration change control, that:

> The organization:
>
> a. Determines the types of changes to the information system that are configuration controlled;

[5] Recommendation 9, Audit of the Millennium Challenge Corporation's Compliance with Provisions of the Federal Information Security Management Act for Fiscal Year 2010," (Audit Report No. M-000-10-004-P), August 31, 2010.

Control Enhancement:

* * *

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

Without properly testing and approving changes to systems and application software there is an increased risk of back doors, Trojans, and other malicious code exposing MCC's computer resources to intentional and unintentional loss or impairment, destruction or malicious damage. Therefore, we recommend the following:

Recommendation 14: *We recommend that the Millennium Challenge Corporation Chief Information Officer re-open recommendation 9 in Office of Inspector General Audit Report No. M-000-10-004-P.*

9. MCC Needs to Periodically Test Contingency Plans

MCC had not performed testing of the MCCNet contingency plan for fiscal year 2012. The last test was conducted in February of 2011; however, the test results and lessons learned were not formally documented and reported until November 2011. MCC delayed testing of the contingency plan in fiscal year 2012 due to the data center migration to Terremark in Culpeper, Virginia. Contingency plan testing was scheduled to be performed in August 2012; however, testing had not occurred for over one calendar year.

MCC's *Information Systems Security Policy* states: "System administrators must annually test contingency plans, document results, and recommend improvements. System owners must test the contingency plan for their system at least annually using the CISO-defined standard tests and document the results."

NIST Special Publication 800-53, Revision 3, security control CP-4 states the following regarding contingency plan testing and exercises:

The organization:

a. Tests and/or exercises the contingency plan for the information system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests and/or exercises*] to determine the plan's effectiveness and the organization's readiness to execute the plan; and,
b. Reviews the contingency plan test/exercise results and initiates corrective actions.

Lack of contingency plan testing increases the likelihood that the contingency plans in place will not function appropriately. Additionally, the data center move increases the risk of contingency plan failure due to new and untested logistical requirements. As a result, we recommend the following:

Recommendation 15: *We recommend that Millennium Challenge Corporation Chief Information Officer implement a documented validation process to ensure the annual testing of contingency plans and timely reporting of lessons learned, as required by the* Information System Security Policy*.*

10. MCC Needs to Assess and Update Security Policies

As a result of the prior year FISMA audit recommendation,[6] the MCC Chief Information Security Office developed the *MCC Information Systems Policy Review Process* document that includes reviewing and updating the MCC *Information System Security Policy* annually to ensure it addresses guidance from NIST, specifically Special Publication 800-53, Revision 3. Based on our review this year, MCC had not fully implemented NIST Special Publication 800-53, Revision 3 into the Corporation's information system security policies. MCC was in the process of updating the Policy; however, it had not been finalized.

Management indicated that the updating of policies was delayed because the Chief Information Security Office was focused on remediating other audit findings and the continuing data center transfer.

NIST Special Publication 800-53, Revision 3, security control PL-1, states the following regarding security planning policy and procedures:

> The organization develops, disseminates, and reviews/updates [*Assignment: organization defined frequency*]:
>
> a. A formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
> b. Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.

Without updating information system security policies to reflect current security control standards and environment, MCC's information systems may be more susceptible to new and heightened security risks. Therefore, we recommend the following:

> ***Recommendation 16:*** *We recommend that the Millennium Challenge Corporation Chief Information Officer re-open recommendation 9 in Office of Inspector General Audit Report No. M-000-11-004-P.*

11. MCC Needs to Update the MCCNet System Security Plan

The MCCNet System Security Plan did not accurately reflect the current information system environment. For example:

- All contingency planning controls were noted as planned controls; however, these controls are in place.
- Personnel security controls 3, 4, 5, 6, 7, and 8 state that these controls were provided by the Office of Security; however, there was no description of the controls implemented.

[6] Recommendation 9, "Audit of the Millennium Challenge Corporation's Compliance with the Federal Information Security Management Act of 2002 – Fiscal Year 2011," (Report No. M-000-11-004-P), September 27, 2011.

- There was no reference to the USAID Interconnection Security Agreement and Memorandum of Understanding. However, the system security plan was updated during the audit to reflect this reference after identification.

NIST Special Publication 800-53, Revision 3 security control PL-2, states the following regarding system security plans:

> The organization:
> * * *
> b. Reviews the security plan for the information system [*Assignment: organization-defined frequency*];
> c. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.

In response to a prior FISMA audit recommendation[7], MCC developed an Internal System Review Process to ensure that internal systems are reviewed on an annual basis, which includes reviewing system security plans. Although MCC closed that recommendation, MCC management had not updated the system security plan to reflect the current system environment. This was a result of management oversight in updating the MCCNet system security plan.

Without a complete and current system security plan, security responsibilities and controls are not appropriately documented, disseminated, implemented, or monitored; therefore, MCCNet may be more susceptible to improper access, use, or loss of sensitive information. Therefore, we recommend the following:

> ***Recommendation 17:*** *We recommend that the Millennium Challenge Corporation Chief Information Officer re-open recommendation 10 in Office of Inspector General Audit Report No. M-000-11-004-P.*

12. MCC Needs to Strengthen Risk Management Controls

As a result of a previous audit,[8] a recommendation was made for MCC to implement a process to verify that risk management plans and Exhibit 300 business cases are consistently used, monitored and updated annually for all information technology projects. However, MCC had not updated the MIDAS exhibit 300 to identify required resources. MCC was planning to release an updated version of MIDAS during fiscal year 2012; however, the exhibit 300 was not updated to reflect the change.

Additionally, the MCC Information System Security Policy did not adequately address security and risk management in relation to enterprise architecture. This was partially

[7] Recommendation 10, "Audit of the Millennium Challenge Corporation's Compliance with the Federal Information Security Management Act of 2002 – Fiscal Year 2011," (Report No. M-000-11-004-P), September 27, 2011.

[8] Recommendation 13, "Risk Assessment of the Millennium Challenge Corporation's Information Technology Governance Over its Information Technology Investments Report" (Audit Report No. M-000-11-001-O), May 13, 2011.

due to MCC not fully implementing NIST Special Publication 800-53, Revision 3 as well as risk management guidelines, such as those contained in NIST Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*.

NIST Special Publication 800-53, Revision 3, security control PM-7, states the following regarding enterprise architecture: The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation."

Additionally, security control PM-3 states the following regarding the information security resources:

> The organization:
>
> a. Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement;
> b. Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and,
> c. Ensures that information security resources are available for expenditure as planned.

The lack of risk management controls for enterprise architecture may increase the difficulty the agency has managing IT projects and assets.

A recommendation addressing part of this finding was made in a previous audit;[9] however, procedures had not been fully implemented prior to MCC management's closure of the prior year recommendation. Therefore, we recommend the following. (We have not made additional recommendations since the remaining issues were reported in a previous audit and MCC has not yet taken final actions to address all weaknesses.)[10]

> ***Recommendation 18:*** *We recommend that the Millennium Challenge Corporation Chief Information Officer re-open recommendation 13 in Office of Inspector General Audit Report No.* M-000-11-001-O*.*

[9] Recommendation 13, "Risk Assessment of the Millennium Challenge Corporation's Information Technology Governance Over its Information Technology Investments Report" (Audit Report No. M-000-11-001-O), May 13, 2011.

[10] Recommendations 2 and 6, "Risk Assessment of the Millennium Challenge Corporation's Information Technology Governance Over its Information Technology Investments Report" (Audit Report No. M-000-11-001-O), May 13, 2011.

EVALUATION OF MANAGEMENT COMMENTS

In response to the draft report, the Millennium Challenge Corporation (MCC) outlined its plans to address all 18 audit recommendations and described planned actions to address the recommendations. MCC's comments are included in their entirety in Appendix II.

For Recommendation 1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 13, 14, 15, 16, 17 and 18, MCC described and outlined its plans to address the audit recommendations and provided target dates for when the final actions would be completed. We agree with MCC's management decisions for those recommendations. Although MCC's management decisions for Recommendation 9 and 12 were not fully responsive, as discussed below, we are accepting MCC's planned action.

In response to Recommendation 9, MCC indicated that its Chief Information Officer will work with the MCC Chief Information Security Officer to update the "MCC Annual System Review Process" to ensure system risk assessments are reviewed and updated on an annual basis. We are accepting MCC's planned action because MCC currently has a policy to review and update risk assessments on an annual basis; however, they were not performing them in accordance with the policy. As a result, the corrective action addresses the implementation of the recommendation.

In response to Recommendation 12, MCC indicated that they will document and implement reporting metrics to monitor user participation and criteria for accepting Tip of the Day participation as annual security awareness training. We are accepting MCC's planned action because the reporting metrics will enable MCC to track and validate that all employees and contractors receive annual security awareness training. As a result, the corrective action addresses the implementation of the recommendation.

APPENDIX I

SCOPE AND METHODOLOGY

Scope

We conducted this audit 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 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 minimum security controls for selected information systems to meet the Federal Information Security Management Act of 2002 to reduce the risk of data tampering, unauthorized access to and disclosure of sensitive information, and disruption to MCC's operations.

The audit included the testing of selected management, technical, and operational controls outlined in National Institute of Standards in Technology Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations, August 2009, Revision 3* to assess MCC's performance and compliance with FISMA in the following areas:

- Access Controls
- Awareness and Training
- Security Assessment and Authorization
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Media Protection
- Physical and Environmental
- Program Management
- System and Communications Protection
- System and Information Integrity

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 correcting/mitigating technical vulnerabilities. In addition, the audit included a follow up on prior year audit recommendations[11] to determine if MCC had made progress in implementing the recommended improvements concerning its information security program.

At time of the audit, MCC's system inventory included one internal system, MCCNet general support system; one internal major application, MCC Integrated Data Analysis

[11] "Audit of the Millennium Challenge Corporation's Compliance with Provisions of the Federal Information Security Management Act for Fiscal Year 2010," (Audit Report No. M-000-10-004-P), August 31, 2010 and "Audit of the Millennium Challenge Corporation's Compliance with Provisions of the Federal Information Security Management Act for Fiscal Year 2011," (Audit Report No. M-000-11-004-P), September 27, 2011.

System (MIDAS); and seven third-party major applications: (1) National Business Center Oracle Federal Financials, (2) National Business Center Federal Personnel and Payroll System, (3) e-Official Personnel Folder, (4) e-Travel, (5) MCC Public Website, (6) International Treasury Services, and (7) MCC Contract Management System. The scope of this audit was primarily on the two systems operated by MCC. In addition, selected controls for external systems were reviewed as well.

The audit fieldwork was performed at the Millennium Challenge Corporation's headquarters in Washington, D.C., from May 4, 2012, to August 8, 2012.

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) identification and authentication policies and procedures; and (5) change control documentation. Where appropriate, we compared documents, such as the IT policies and procedures, to requirements stipulated by the National Institute of Standards and Technology (NIST) 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 reviewing 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 report recommendations for FY 2010[12] and FY 2011.[13]

[12] "Audit of the Millennium Challenge Corporation's Compliance with Provisions of the Federal Information Security Management Act for Fiscal Year 2010," (Audit Report No. M-000-10-004-P), August 31, 2010.

[13] "Audit of the Millennium Challenge Corporation's Compliance with Provisions of the Federal Information Security Management Act for Fiscal Year 2011," (Audit Report No. M-000-11-004-P), September 27, 2011.

Appendix II

MANAGEMENT COMMENTS

September 26, 2012

MEMORANDUM TO: **Richard Taylor**
Assistant Deputy Inspector General for the Millennium Challenge Corporation

FROM: **Paul S. Malone /s/**
Chief Information Officer
Millennium Challenge Corporation

SUBJECT: **MCC Comments on the Millennium Challenge Corporation's Compliance with the Federal Information Security Management Act of 2002 - FY 2012**

The Millennium Challenge Corporation (MCC) appreciates the opportunity to comment on the Fiscal Year 2012 audit of MCC's compliance with the regulatory requirements of the Federal Information Security Management Act of 2002 (FISMA).

We appreciate the opportunity to respond to your audit recommendations and consider your role vital in helping to achieve and sustain our FISMA compliance.

Our Management Response to your recommendations follows.

Recommendation No. 1: We recommend that the Millennium Challenge Corporation Chief Information Officer establish patch timeframe requirements to ensure remediation of known vulnerabilities.

Management Response: MCC concurs with this recommendation. The MCC Chief Information Officer will work with the MCC Operations and Maintenance provider to update the "MCC Operations Vulnerability Management Process" to define a timeframe within which O&M must apply patches for known vulnerabilities or document why the patches cannot be applied, by January 31, 2013. This constitutes MCC's Management Decision.

Recommendation No. 2: We recommend that the Millennium Challenge Corporation Chief Information Officer review the critical and high risk vulnerabilities identified by the Office of Inspector General contractor and document why the vulnerabilities are not

being identified by the Corporation's vulnerability management tool.

Management Response: MCC concurs with this recommendation. The MCC Chief Information Officer will review the critical and high vulnerabilities identified by the OIG scanning tool and determine if nCircle detected a similar vulnerability and, if not, work with nCircle to determine and document why they were not detected, by November 30, 2012. This constitutes MCC's Management Decision.

Recommendation No. 3: We recommend that the Millennium Challenge Corporation Chief Information Officer document and implement a process for documenting management review, acceptance and corresponding compensating controls for known vulnerability scan exclusions.

Management Response: MCC concurs with this recommendation. The MCC Chief Information Officer will document and implement a process for documenting management review and acceptance of vulnerability signatures excluded from vulnerability scans, by December 31, 2012. This constitutes MCC's Management Decision.

Recommendation No. 4: We recommend that the Millennium Challenge Corporation Chief Information Officer document and implement a process to conduct periodic reviews, as defined by the Corporation, of MCCNet users to verify that appropriate access privileges have been assigned.

Management Response: MCC concurs with this recommendation. The MCC Chief Information Officer will work with the MCC Operations and Maintenance provider to document and implement a process to conduct periodic reviews of MCCNet user accounts to verify that appropriate access privileges have been assigned, by November 30, 2012. This constitutes MCC's Management Decision.

Recommendation No. 5: We recommend that the Millennium Challenge Corporation Chief Information Officer document and implement a process to review active accounts that have never logged into the system to determine whether accounts are necessary.

Management Response: MCC concurs with this recommendation. The MCC Chief Information Officer will document and implement a process to review active MCCNet accounts that have never logged into the system to determine whether accounts are necessary, by January 31, 2013. This constitutes MCC's Management Decision.

Recommendation No. 6: We recommend that the Millennium Challenge Corporation 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 ensure its implementation.

Management Response: MCC concurs with this recommendation. The MCC Vice President of Administration and Finance will document and implement a process to perform periodic, as defined by the Corporation, reviews of the exit clearance process to ensure its implementation, by February 28, 2013. This constitutes MCC's Management Decision.

Recommendation No. 7: We recommend that the Millennium Challenge Corporation Chief Information Officer conduct a full system reauthorization for MCCNet in accordance with Corporation's policy.

Management Response: MCC concurs with this recommendation. The MCC Chief Information Officer will conduct a full system reauthorization for the MCCNet General Support System, by March 31, 2013. This constitutes MCC's Management Decision.

Recommendation No. 8: We recommend that the Millennium Challenge Corporation Chief Information Officer implement a documented validation process to ensure security impact assessments are conducted prior to significant system changes in accordance with the Corporation's policy.

Management Response: MCC concurs with this recommendation. The MCC Chief Information Officer will work with the MCC Chief Technology Officer and the MCC Chief Security Officer to update the Change Control Procedures to document a validation process to ensure security impact assessments are conducted prior to significant system changes, by February 28, 2013. This constitutes MCC's Management Decision.

Recommendation No. 9: We recommend that the Millennium Challenge Corporation Chief Information Officer implement a documented validation process to ensure system risk assessments are reviewed and updated on an annual basis, as required by the Information System Security Policy.

Management Response: MCC concurs with this recommendation. The MCC Chief Information Officer will work with the MCC Chief Information Security Officer to update the "MCC Annual System Review Process" to ensure system risk assessments are reviewed and updated on an annual basis, by December 31, 2012. This constitutes MCC's Management Decision.

Recommendation No. 10: We recommend that Millennium Challenge Corporation Chief Information Officer document and implement a continuous monitoring plan to assess an appropriate number of controls for the agency's information systems on a Corporation-defined frequency.

Management Response: MCC concurs with this recommendation. The MCC Chief Information Officer will work with the MCC Chief Information Security Officer to update the "MCC Annual System Review Process" to document and implement a continuous monitoring plan to assess, at a defined frequency, an appropriate number of security controls for each agency system, by December 31, 2012. This constitutes MCC's Management Decision.

Recommendation No. 11: We recommend that the Millennium Challenge Corporation Chief Information Security Officer document and implement metrics for accepting Tip of the Day participation as annual security awareness training.

Management Response: MCC concurs with this recommendation. The MCC Chief Information Security Officer will document and implement reporting metrics to monitor user participation and criteria for accepting Tip of the Day participation as annual security awareness training, by November 30, 2012. This constitutes MCC's Management Decision.

Recommendation No. 12: We recommend that the Millennium Challenge Corporation Chief Information Security Officer document and implement a process to track and validate that all employees and contractors receive the annual security awareness training through either the Tips of the Day program or by taking another acceptable security awareness training.

Management Response: MCC concurs with this recommendation. The MCC Chief Information Security Officer will document and implement reporting metrics to monitor user participation and criteria for accepting Tip of the Day participation as annual security awareness training, by November 30, 2012. This constitutes MCC's Management Decision.

Recommendation No. 13: We recommend that the Millennium Challenge Corporation Chief Information Officer document and implement asset management procedures to include processes for ensuring information system assets are tracked appropriately, and that periodic, as defined by the Corporation, information system asset inventories are performed.

Management Response: MCC concurs with this recommendation. The MCC Chief Information Officer will work with the MCC Operations and Maintenance provider to document and implement asset management procedures to include processes for ensuring information system assets are tracked appropriately and that periodic information system asset inventories are performed, by April 30, 2013. This constitutes MCC's Management Decision.

Recommendation 14: We recommend that the Millennium Challenge Corporation Chief Information Officer re-open Recommendation 9 in Office of Inspector General Audit Report No. M-000-10-004-P.

Management Response: MCC concurs with this recommendation and will re-open Recommendation 9 in Audit Report No. M-000-10-004-P. The MCC Chief Information Officer will document, disseminate, and implement Configuration Management Procedures as defined in NIST SP 800-53r3, by April 30, 2013 and will track progress using this recommendation. This constitutes MCC's Management Decision.

Recommendation No. 15: We recommend that Millennium Challenge Corporation Chief Information Officer implement a documented validation process to ensure the annual testing of contingency plans and timely reporting of lessons learned, as required by the Information System Security Policy.

Management Response: MCC concurs with this recommendation. The MCC Chief Information Officer will implement a documented validation process to ensure the annual testing of contingency plans and timely reporting of lessons learned, by March 31, 2013. This constitutes MCC's Management Decision.

Recommendation No. 16: We recommend that the Millennium Challenge Corporation Chief Information Officer re-open recommendation 9 in Office of Inspector General Audit Report No. M-000-11-004-P.

Management Response: MCC concurs with this recommendation and will re-open Recommendation 9 in Audit Report No. M-000-11-004-P. The MCC Chief Information Officer will develop and implement a documented process to review and update the Information System Security Policy to address NIST SP 800-53r3, by December 31, 2012 and will track progress using this recommendation. This constitutes MCC's Management Decision.

Recommendation No. 17: We recommend that the Millennium Challenge Corporation Chief Information Officer re-open recommendation 10 in Office of Inspector General Audit Report No. M-OOO-11-004-P.

Management Response: MCC concurs with this recommendation and will re-open Recommendation 10 in Audit Report No. M-000-11-004-P. The MCC Chief Information Officer will work with the MCC Chief Information Security Officer to update the "MCC Annual System Review Process" to review and update System Security Plans on an annual basis to ensure that the security requirements and controls for the system are adequately documented and reflect the current information system environment, by November 30, 2012 and will track progress using this recommendation. This constitutes MCC's Management Decision.

Recommendation No. 18: We recommend that the Millennium Challenge Corporation Chief Information Officer re-open recommendation 13 in Office of Inspector General Audit Report No. M-000-11-001-0.

Management Response: MCC concurs with this recommendation and will re-open Recommendation 13 in Audit Report No. M-000-11-001-O.The MCC Chief Information Officer will implement a process to verify that risk management plans and Exhibit 300 business cases are consistently used, monitored and updated annually for all information technology projects, by February 28, 2013 and will track progress using this recommendation. This constitutes MCC's Management Decision.

If you have any questions, comments or concerns please feel free to contact me on 202.521.3672.

CC: IG/MCC, Lisa Banks
IG/MCC, Aleta Johnson
MCC/A&F/FMD, Arlene McDonald

Appendix III

Status of Prior Year Findings[14]

No.	Recommendation	MCC Status	Auditor's Position on Status
1	2011 Recommendation No. 1: We recommend that the Millennium Challenge Corporation Chief Information Officer review vulnerability scans performed by the Office of Inspector General contractor and document action taken to appropriately mitigate identified vulnerabilities or appropriately document the business need and acceptance of risk of uncorrected vulnerabilities.	Closed	Closed
2	2011 Recommendation No. 2: We recommend that the Millennium Challenge Corporation Chief Information Officer develop and implement a documented process to ensure all agency computers are scanned for malicious code.	Closed	Closed
3	2011 Recommendation No. 3: We recommend that the Millennium Challenge Corporation Chief Information Officer develop and implement a documented process to ensure all devices attached to the network are included in vulnerability scans.	Closed	Closed
4	2011 Recommendation No. 4: We recommend that the Millennium Challenge Corporation Chief Information Officer develop and implement a documented process for ensuring the encryption of backup data prior to transferring offsite.	Closed	Closed
5	2011 Recommendation No. 5: We recommend that the Millennium Challenge Corporation Chief Information Officer develop and implement a documented process to test backup tapes and document the results of backup restorations.	Closed	Closed
6	2011 Recommendation No. 6: We recommend that the Millennium Challenge Corporation Chief Information Officer define in the Information System Security Policy a specific frequency for testing backup information to verify media reliability and information integrity.	Closed	Closed
7	2011 Recommendation No. 7: We recommend that the Millennium Challenge Corporation Chief Information Officer re-open recommendation 5 in Office of Inspector General Audit Report No. M-000-10-004-P. 2010 Recommendation No. 5: We recommend that the Millennium Challenge Corporation Chief Information Officer work with the Office of Security and the Office of	Closed	Closed

[14] "Audit of the Millennium Challenge Corporation's Compliance with Provisions of the Federal Information Security Management Act for Fiscal Year 2011," (Audit Report No. M-000-11-004-P), September 27, 2011.

No.	Recommendation	MCC Status	Auditor's Position on Status
	Human Resources to review the termination process to determine why it broke down, develop and implement a control to correct the weakness identified and revise the policy accordingly to reflect the new process.[15]		
8	2011 Recommendation No. 8: We recommend that the Millennium Challenge Corporation Chief Information Officer implement and document a process to conduct periodic reviews of MCCNet user accounts to identify and disable unnecessary accounts.	Closed	Closed
9	2011 Recommendation No. 9: We recommend that the Millennium Challenge Corporation Chief Information Officer develop and implement a documented process to review and update the Information System Security Policy to address National Institute of Standards and Technology Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations.	Closed	Open. FY 2011 FISMA Audit noted weaknesses. Please refer to Finding #10.
10	2011 Recommendation No. 10: We recommend that the Millennium Challenge Corporation Chief Information Officer develop and implement a documented process to review and update System Security Plans on an annual basis to ensure that the security requirements and controls for the system are adequately documented and reflect the current information system environment.	Closed	Open. FY 2011 FISMA Audit noted weaknesses. Please refer to Finding #11.
11	2011 Recommendation No. 11: We recommend that the Millennium Challenge Corporation Chief Information Officer either: • Develop and implement a documented process to conduct annual security control assessments for the agency's information systems, as required by the Information System Security Policy; or, • Review and revise the Information System Security Policy to reflect the current management position regarding the required frequency of system security assessments.	Closed	Closed
12	2011 Recommendation No. 12: We recommend that the Millennium Challenge Corporation Chief Information Officer develop and implement a documented process to maintain up-to-date plans of action and milestones and implement corrective actions in a timely manner.	Closed	Closed
13	2011 Recommendation No. 13: We recommend that the Millennium Challenge Corporation Chief Information Officer re-open recommendation 9 in Office of Inspector General Audit Report No. M-000-10-004-P.	Closed	Open. FY 2011 FISMA Audit noted weaknesses. Please refer to Finding #8.

[15] "Audit of the Millennium Challenge Corporation's Compliance with Provisions of the Federal Information Security Management Act for Fiscal Year 2010," (Audit Report No. M-000-10-004-P), August 31, 2010.

No.	Recommendation	MCC Status	Auditor's Position on Status
	2010 Recommendation No. 9: We recommend that the Millennium Challenge Corporation Chief Information Officer document, disseminate and implement Configuration Management Procedures.[16]		

[16] "Audit of the Millennium Challenge Corporation's Compliance with Provisions of the Federal Information Security Management Act for Fiscal Year 2010," (Audit Report No. M-000-10-004-P), August 31, 2010.

Summary of Results of Each Control Reviewed

Control #	Control Name	Is Control Effective? (Yes/No)
MCCNET		
AT-1	Security Awareness & Training Policy and Procedures	Yes
AT-2	Security Awareness	No, See Finding 6
AT-3	Security Training	Yes
AT-4	Security Training Records	Yes
PE-1	Physical &Environmental Protection Policy and Procedures	Yes
PE-2	Physical Access Authorizations	Yes
PE-3	Physical Access Control	Yes
PE-4	Access Control for Transmission Medium	Yes
PE-5	Access Control for Output Devices	Yes
PE-6	Monitoring Physical Access	Yes
PE-7	Visitor Control	Yes
PE-8	Access Records	Yes
PE-9	Power Equipment & Power Cabling	Yes
PE-10	Emergency Shutoff	Yes
PE-11	Emergency Power	Yes
PE-12	Emergency Lighting	Yes
PE-13	Fire Protection	Yes
PE-14	Temperature & Humidity Controls	Yes
PE-15	Water Damage Protection	Yes
PE-16	Delivery & Removal	Yes
PE-17	Alternate Work Site	Yes
PE-18	Location of Information System Components	Yes
CA-1	Security Assessment and Authorization Policy & Procedures	Yes
CA-2	Security Assessments	No, See Findings 4, 5, & 10
CA-3	Information System Connections	No, See Finding 11
CA-5	Plan of Action and Milestones	Yes
CA-6	Security Authorization	No, See Finding 4
CA-7	Continuous Monitoring	No, See Finding 5
CP-1	Contingency Planning Policy & Procedures	Yes
CP-2	Contingency Plan	Yes
CP-3	Contingency Training	Yes
CP-4	Contingency Plan Testing and Exercises	No, See Finding 9
CP-6	Alternate Storage Sites	Yes
CP-7	Alternate Processing Sites	Yes
CP-8	Telecommunication Services	Yes
CP-9	Information System Backup	Yes
CP-10	Information System Recovery & Reconstitution	Yes
RA-1	Risk Assessment Policy and Procedures	Yes

RA-2	Security Categorization	Yes
RA-3	Risk Assessment	No, See Finding 4
RA-5	Vulnerability Scanning	No, See Finding 1
SC-7	Boundary Protection	Yes
SC-28	Protection of Information at Rest	Yes
SI-2	Flaw remediation	Yes
PM-1	Information Security Program Plan	No, See Finding 10
PM-3	Information Security Resources	No, See Finding 12
PM-4	Plan of Action and Milestones Process	Yes
PM-5	Information System Inventory	Yes
PM-6	Information Security Measures of Performance	Yes
PM-7	Enterprise Architecture	No, See Finding 12
PM-9	Risk Management Strategy	Yes
PM-10	Security Authorization Process	Yes
AC-1	Access Control Policy & Procedures	Yes
AC-2	Account Management	No, See Findings 2 & 3
AC-3	Access Enforcement	Yes
AC-4	Information Flow Enforcement	Yes
AC-5	Separation of Duties	Yes
AC-6	Least Privilege	Yes
AC-7	Unsuccessful Login Attempts	Yes
AC-17	Remote Access	Yes
AC-18	Wireless Access	Yes
AC-19	Access Control for Mobile Devices	Yes
AC-20	Use of External Information Systems	Yes
CM-1	Configuration Management Policy and Procedures	No, See Finding 8
CM-2	Baseline Configuration	Yes
CM-3	Configuration Change Control	No, See Finding 8
CM-6	Configuration Settings	Yes
CM-7	Least Functionality	Yes
CM-8	Information System Component Inventory	No, See Finding 7
CM-9	Configuration Management Plan	No, See Finding 8
IA-1	Identification and Authentication Policy and Procedures	Yes
IA-2	Identification and Authentication (Organizational Users)	Yes
IA-3	Device Identification and Authentication	Yes
IA-5	Authenticator Management	Yes
IR-1	Incident Response Policy and Procedures	Yes
IR-2	Incident Response Training	Yes
IR-3	Incident Response Testing and Exercises	Yes
IR-4	Incident Handling	Yes
IR-5	Incident Monitoring	Yes
IR-6	Incident Reporting	Yes
IR-7	Incident Response Assistance	Yes
IR-8	Incident Response Plan	Yes
MP-1	Media Protection Policies and Procedures	Yes
MP-2	Media Access	Yes
MP-3	Media Marking	Yes
MP-4	Media Storage	Yes

MP-5	Media Transport	Yes
MP-6	Media Sanitization	Yes
MIDAS		
RA-2	Security Categorization	Yes
RA-3	Risk Assessment	No, See Finding 4
National Business Center Oracle Federal Financials		
RA-2	Security Categorization	Yes
RA-3	Risk Assessment	Yes
MCC Public Website		
RA-2	Security Categorization	Yes
RA-3	Risk Assessment	Yes
AC-22	Public Accessibility Content	Yes
E2 Travel Solutions		
RA-2	Security Categorization	Yes
RA-3	Risk Assessment	Yes
Electronic Official Personnel File		
RA-2	Security Categorization	Yes
RA-3	Risk Assessment	Yes
National Business Center Federal Personnel and Payroll System		
RA-2	Security Categorization	Yes
RA-3	Risk Assessment	Yes
Contracts and Grants Management System		
RA-2	Security Categorization	Yes
RA-3	Risk Assessment	Yes

U.S. Agency for International Development
Office of Inspector General
1300 Pennsylvania Ave, NW
Washington, DC 20523
Tel: (202) 712-1150
Fax: (202) 216-3047
www.usaid.gov/oig