



**OFFICE OF INSPECTOR GENERAL
MILLENNIUM CHALLENGE CORPORATION**

**MCC'S IMPLEMENTATION OF
EXECUTIVE ORDER 13526,
CLASSIFIED NATIONAL
SECURITY INFORMATION,
NEEDS STRENGTHENING**

REVIEW REPORT NO. M-000-16-001-S
SEPTEMBER 30, 2016

WASHINGTON, DC



Office of Inspector General

September 30, 2016

Mr. Douglas Fairfield
Managing Director, Domestic and International Security
Millennium Challenge Corporation
1099 14th Street, NW 7th Floor
Washington, DC 20005

Dear Mr. Fairfield:

This letter transmits the Office of Inspector General's review report, "MCC's Implementation of Executive Order 13526, Classified National Security Information, Needs Strengthening" (M-000-16-001-S). In finalizing the report, we considered your written comments on our draft and included those comments in their entirety in appendix II.

The report contains one recommendation. We acknowledge MCC's management decision on it.

Thank you and your staff for the cooperation and assistance extended to us during this review.

Sincerely,

/s/

Thomas E. Yatsco
Assistant Inspector General for Audit

cc: Jim Blades, Acting Vice President, Contracts and Administration, Department of
Administration and Finance
Jude Koval, Director of Internal Controls and Audit Compliance
Karla L. Chryar, Compliance Officer, Internal Controls and Audit Compliance

INTRODUCTION

The Reducing Over-Classification Act, Public Law 111-258, was enacted in October 2010 to prevent overclassification of information and promote sharing information within the Federal Government; with State, local, and tribal entities; and with the private sector. It followed President Barack Obama's December 2009 Executive Order 13526, "Classified National Security Information," which "prescribes a uniform system for classifying, safeguarding and declassifying national security information." According to the order, "Protecting information critical to our Nation's security and demonstrating our commitment to open Government through accurate and accountable application of standards and routine, secure, and effective declassification are equally important priorities."

The act requires inspectors general to produce two reports on their agencies' compliance with classification policies, procedures, rules, and regulations. This review is the second of the two required reports by the Office of Inspector General (OIG) for the Millennium Challenge Corporation (MCC). We issued the first, "Evaluation of Millennium Challenge Corporation's Implementation of Executive Order 13526, Classified National Security Information (M-000-15-001-S)," on December 18, 2014.

OIG conducted this review to do the following:

1. Identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material at MCC.
2. Assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered at MCC.
3. Determine whether MCC addressed recommendations OIG made in its previous report.

To conduct our work, we reviewed classified national security information activities since OIG's first evaluation; examined MCC policies, regulations, and procedures; and interviewed MCC officials. In addition, we reviewed corrective actions taken in response to recommendations in our previous report. Additional details about our scope and methodology are in appendix I. We conducted this review following internally established policies.

SUMMARY

For board meetings that took place from December 10, 2013, through December 16, 2015, MCC classified the transcripts and minutes at the proper level. We did not find evidence of persistent misclassification of material at MCC.

However, we found that MCC's classified national security information program does not fully meet the requirements of Executive Order 13526 or the Code of Federal Regulations (32 CFR Part 2001). MCC's policies and procedures omit key requirements. Additionally, MCC did not effectively conduct a self-inspection program in fiscal year 2015. Individuals with original classification authority, including two who classified documents, did not receive the required annual training, and not all staff completed the required annual refresher training. In addition, despite classifying at the right level, MCC does not have documented policies and procedures

for classifying board meeting transcripts and minutes, nor does it have written procedures for providing access to Department of State cables, or maintaining a security incident log.

Further, MCC's implementation of recommendations in our 2014 report was inadequate. Although MCC reported taking final action on all four of the recommendations, we found some of the same problems again in this review, indicating that the corrective actions were not all effective.

To address these problems, we recommend that the Domestic and International Security Division, in coordination with the Office of General Counsel, implement a corrective action plan addressing OIG's review results. Doing so would strengthen MCC's classified national security information program and help the agency achieve full compliance with both Executive Order 13526 and the regulations and directives of the National Archives and Records Administration's Information Security Oversight Office (ISOO).

BACKGROUND

Executive Order 13526 designates ISOO to issue directives that all agencies must follow, and to oversee agency actions to ensure compliance with the order. ISOO issues its standards through Title 32 of the Code of Federal Regulations, Part 2001, "Classified National Security Information," which directs agencies with original classification authority, like MCC, to implement policies and procedures for their programs. The regulation establishes standards for classifying, declassifying, marking, and safeguarding information; conducting self-inspection programs and security education and training; and issuing classification and declassification guides.

There are two types of classification: original and derivative. According to the Executive order, original classification involves making an "initial determination that information requires, in the interest of national security, protection against unauthorized disclosure." The State Department's Foreign Affairs Manual defines derivative classification as "reproducing, extracting, or summarizing classified information, or applying classification markings derived from source material or as directed by a classification guide." Three positions at MCC have original classification authority up to the secret level. During OIG's first evaluation, and until December 23, 2014, the three positions were the chief executive officer, the vice president and chief counsel, and the vice president of the Department of Compact Operations. After December 23, 2014, the positions were the chief executive officer, the vice president and chief counsel, and the Domestic and International Security Division's managing director.

According to MCC officials, MCC has never originally classified information, and its derivatively classified information consists solely of transcripts and minutes of its board of directors meetings. Officials said they derive these documents' classifications based on source documents or, as OIG found in its testing, a State Department classification guide. MCC reported 87 classified transcripts and meeting minutes in its inventory as of December 9, 2015—most marked confidential, although some were marked secret.

OIG's prior evaluation found instances of noncompliance in MCC's classified national security information program regarding classification markings, security training, and the lack of specific guidance covering training requirements for both those with original classification authority and all employees. To address these concerns, OIG recommended that MCC verify compliance with marking requirements in specific instances, document that all its original classification

authorities completed required trainings or obtained waivers, and establish formal guidance requiring documentation of completion by all employees, including original classifiers, of Executive order training requirements.

REVIEW RESULTS

MCC Classified Information at the Proper Level

MCC had 18 classified documents from board meetings held December 10, 2013, through December 16, 2015. MCC said that the documents were derivatively classified by the Department of State's classification guidelines. We confirmed that the classification blocks were completed and cited guidelines sections that related to: (1) foreign relations or foreign activities of the United States, including confidential sources, (2) scientific, technological, or economic matters relating to national security, and (3) intelligence activities, including covert action, intelligence sources or methods, or cryptology. Our review did not find evidence of persistent misclassification of material at MCC.

MCC's Classified National Security Information Program Does Not Fully Comply With Executive Order 13526 and Information Security Oversight Office Regulations and Directives

We found that MCC did not fully comply with Executive Order 13526 and related regulations and directives. Specifically, we identified weaknesses with program policies and procedures, the self-inspection program, the declassification program, security education and training, classification markings, and the documentation of some internal controls for managing classified information.

Program Policies and Procedures. MCC's guidance and policy regarding classified national security information primarily reside in three documents: (1) a classification guide, (2) a declassification guide, and (3) MCC's policy on providing public sector board members' plus ones access to confidential information.¹ These policies and procedures do not cover the following aspects of Executive Order 13526 and 32 CFR Part 2001:

- Trainings required for derivative classifiers and those with original classification authority at MCC, as well as provisions for suspension of original classification authority when training requirements are not met.
- Responsibilities for tracking and monitoring employees' training compliance.
- Provisions for authorized holders of information to challenge its classification if they believe it is improper, along with a statement that employees are protected from retribution if they make such challenges.
- The need for the agency to conduct a fundamental classification guidance review at least once every 5 years.

¹ MCC defines plus ones as special Government employees designated by private sector members of MCC's board of directors to assist with fulfilling their duties on the board.

Additionally, whereas MCC's policy on providing private sector board members and plus ones access to confidential information refers to access to material at the confidential level, the board meetings are conducted at the secret level. In at least one instance, the board meeting transcript and minutes were classified at the secret level. This policy needs to be revised to cover all levels of information that might be shared during a board meeting.

Self-Inspection Program and Reporting. Section 5.4(d)(4) of Executive Order 13526 and 32 CFR 2001.60 require senior agency officials to establish self-inspection programs and report on them annually to the Director of ISOO. Self-inspections involve assessing activities such as classification and declassification actions, procedures for safeguarding material, program management and oversight, procedures for security violations, and training.

MCC did not conduct a formal self-inspection in fiscal year 2015. Furthermore, MCC's responses in the report it submitted to ISOO for fiscal year 2015 contained the following errors and inconsistencies:

- Inconsistent statements about how its self-inspection program is administered and how often it is conducted.
- An erroneous statement that MCC's trainings covered the right of an authorized holder to challenge the classification status of information without fear of retribution.
- Inconsistent statements about how often classified actions take place. For example, MCC reported documents were classified twice a year, when it is actually in conjunction with quarterly meetings.

We noted that MCC was in the process of conducting a self-inspection for fiscal year 2016.

Declassification Program. Executive Order Section 3.5(c) states: "Agencies conducting a mandatory review for declassification shall declassify information that no longer meets the standards for classification under this order. They shall release this information unless withholding is otherwise authorized and warranted under applicable law."

The Code of Federal Regulations (32 CFR 2001.12) states that those with original classification authority should "attempt to determine a date or event that is less than 10 years from the date of original classification and which coincides with the lapse of the information's national security sensitivity," and assign that date or event as the time for declassification. If classifiers are unable to determine a date or event less than 10 years away, they should "assign a declassification date that is 10 years from the date of the original classification decision." "If unable to determine a date . . . of 10 years . . . [classifiers can] assign a declassification date not to exceed 25 years from the date of the original classification decision."² Classified information is automatically declassified on the date established.

MCC officials said that in January 2016 they began reviewing documents that had reached their declassification dates or had been classified for 10 years or more. Previously, MCC had not conducted any reviews that assessed whether classified documents should be declassified or

² 2001.12 (a)(i) and (iii).

extended. According to one official, MCC does not have a declassification policy, but plans to create one that will cover review procedures. Not regularly reviewing its classified documents increases the risk of having documents classified longer than necessary.

Security Education and Training. The Code of Federal Regulations (32 CFR Section 2001.70 and Section 2001.71) provides requirements for agencies to implement a training program on the handling of classified information, including the types of trainings, who should attend and how often, and the content of training materials. Those with original classification authority must receive annual training on proper classification and declassification. Failure to complete the training should result in the suspension of their classification authority, unless the agency head grants a waiver. All MCC staff with security clearances must take annual refresher training and may lose their clearance if they do not.

Not all those at MCC with original classification authority took the required training. Six individuals served in these positions in calendar years 2014 and 2015, yet only three took the training. One individual took it in 2014, two others in 2015. None of the individuals had their classification authority suspended, and none received waivers from the agency head. In particular, an individual in the Office of the General Counsel who classified documents during 2014 and 2015 did not take the required training for either year.

MCC provides the annual refresher training through its Web-based SharePoint system. However, the system did not accurately reflect the training status of all employees. The system automatically records the date each person passed the training. The system showed that 27 staff did not complete the training in 2015. A Domestic and International Security Division official explained that some of the staff did not have online access to SharePoint and took the training outside the system. Other staff left MCC in 2015.

Classification Markings. The Code of Federal Regulations (32 CFR Section 2001, Subpart C, "Identification and Markings") requires that markings be uniformly and conspicuously applied so that the information's classified status, classification duration, and level of protection are obvious. MCC's classification guide gives specific instructions about applying the classification markings, such as a classification authority block, declassification instructions, portion markings, and overall classification markings.

We reviewed nine sets of transcripts and minutes covering board meetings held December 10, 2013, through December 16, 2015, for a total of 18 classified documents. Following a board meeting, MCC Office of the General Counsel staff obtain a transcript and use it to draft meeting minutes. The meeting minutes are approved and finalized by the board at the next meeting. The General Counsel officially classifies the transcripts and meeting minutes after board approval.

MCC reports the transcripts and minutes as derivatively classified based on the Department of State's classification guidelines. We found the following:

- All 18 documents contained proper portion markings.
- All 18 documents identified the classifier's name.

- All 18 documents had a declassification date approximately 10 years from the date of classification. However, it was unclear how this date was established: it was not always based on the date of the board meeting or the date the document was classified.
- All nine meeting minutes contained an approval signature, but only one transcript did.
- All nine meeting minutes contained a classification date, but only one transcript was dated.

Documentation of Some Internal Controls for Managing Classified Information. The Government Accountability Office’s “Standards for Internal Control in the Federal Government” states that documentation is a necessary part of an effective internal control system.³ At a minimum, agency management is required to document its internal control system and organization responsibilities. Through multiple interviews with individuals involved in the processes, OIG obtained an understanding of how MCC prepares, handles, and secures classified information and how it tracks and monitors security violations. Below are three examples of important processes related to classified national security information that are not documented at MCC and why they should be.

- *Recording and classifying board meeting transcripts and minutes.* MCC does not have written procedures for recording and classifying board meeting transcripts and minutes. After a board meeting, an Office of the General Counsel paralegal staffer receives a transcript from a certified court reporter contractor who holds a security clearance. The paralegal uses the transcript to create meeting minutes and pencils in initial classified portion markings. At this point, MCC considers the document “unofficially classified.” A member of the Office of the General Counsel refines the draft minutes and gives them and the transcript to the General Counsel, who makes the final decision about classification recommendations. Before the following board meeting, the paralegal arranges for all participating board members to review the draft meeting minutes and suggest any corrections or edits. The General Counsel reviews them again, finalizes them, and presents them at the board meeting for adoption. The General Counsel officially classifies the relevant parts of the adopted minutes, ensuring that the document’s classification blocks are completed properly and setting the date for declassification. The meeting minutes and their accompanying transcripts are then stored in the appropriate container in the MCC security suite. Because these complex procedures involve staff, contractors, board members and their representatives that may experience turnover, a lack of documented procedures increases the risk that classified information could be mishandled or compromised.
- *Accessing Department of State cables.* MCC does not have written procedures for giving access to State Department cables. Currently, a Domestic and International Security Division official sends a daily email to a list of more than 100 individuals in the organization—and the list is growing, as access is not limited. The email lists both classified and unclassified cable titles pertaining to MCC countries of interest. The distribution list has expanded based on requests, and one MCC official we talked to did not see the need to limit its distribution. When individuals ask for access to a classified cable, they are invited to the security suite to read it. Cable copies are shredded at the end of each week. Documentation of these procedures would help MCC analyze potential internal control weaknesses and mitigate risks of classified material being mishandled.

³ GAO-14-704G, September 2014.

- *Maintaining a security incident log.* MCC does not have procedures for maintaining and updating its security incident log, and since the Domestic and International Security Division official who made most of the log entries left the office in May 2015, there has been only 1 entry—compared with 39 for 2014. Examples of past entries in the log include alarms being activated, badges lost, and classified cables returned late. Domestic and International Security Division officials provided differing opinions about when and how to use the log. A lack of a functional security incident log, or an agreement about how one will be structured, not only compromises the agency’s security environment, but also lessens its tracking and enforcement abilities, thus increasing the risk that classified information could be compromised at MCC.

MCC’s Actions on Some of OIG’s Prior Recommendations Were Insufficient

Our 2014 report on MCC’s compliance with Executive Order 13526 made four recommendations to address concerns about the agency’s classified national security information program. MCC reported taking final action on all four recommendations, but we found that corrective actions were not implemented effectively for all of them.⁴

- *Recommendation 1.* One part of the first recommendation was that MCC verify compliance with marking requirements in its annual self-inspection reports. MCC said final action was taken, stating that “self-inspection reports indicating compliance with marking requirements will be verified by ISOO.” However, this response did not address the recommendation to verify compliance. Verification should be done as part of MCC’s self-inspection program. ISOO does not verify agencies’ markings. As part of this review, we found anomalies in classification dates and no supporting documentation for MCC’s assertion in its fiscal year 2015 ISOO report that it checked whether its markings were appropriate.
- *Recommendation 2.* We recommended that MCC document that all original classification authorities have completed the required training or obtain waivers. MCC submitted a training certificate for one individual dated December 23, 2014, but the other individuals did not take original classification authority training in 2014, nor did MCC take actions to prevent training lapses in future years: not all original classification authorities completed their required training in 2015 or obtained waivers.
- *Recommendation 3.* We recommended that MCC establish formal guidance requiring documentation of completion of Executive Order 13526 training requirements for all employees, including original classification authorities. To demonstrate final action, MCC submitted a Department of State cable, “Mandatory Training for Classifiers of National

⁴ After OIG issues a final report containing recommendations, MCC officials and OIG must agree on the course of action to be taken on the recommendations within 6 months. Final action on recommendations occurs when action has been taken to correct or mitigate the problem, or when MCC determines action is not necessary. The action taken must provide reasonable assurance that the deficiency, as described in the finding, has been or is being corrected. MCC determines whether and when final action has occurred. For the remaining two parts of recommendation 1 and for recommendation 4, MCC’s final action addressed the intent of the recommendations.

Security Information,” and referenced a Foreign Assistance Manual provision about training. This action does not address the recommendation. Both the cable and the manual cited the requirement for the training, but did not contain formal guidance on documentation specifically for MCC, tailored to its processes. In this review, we found that MCC did not adequately monitor and document that all staff had completed the required training.

Various factors have contributed to MCC’s insufficient compliance with Federal classified national security information requirements:

- *High turnover of staff.* MCC has experienced high staff turnover agency-wide. Since 2014, the heads of the Domestic and International Security Division and the Office of the General Counsel—primarily responsible for implementing the classified national security information program—have turned over three times. Along with the unexpected turnover of their staff, the turnover of the office heads has strained the agency’s ability to transfer institutional knowledge effectively and maintain adequate program oversight.
- *Misunderstanding of requirements and responsibilities.* A Domestic and International Security Division official mistakenly believed that original classification authority training was required every 2 years and therefore did not verify that MCC officials with original classification authority took annual training. The official also relied on the Office of the General Counsel’s classifications instead of verifying that the markings were appropriate. Further, applicable position descriptions did not include the responsibilities for managing the classified information program.
- *Lack of documented policies and procedures.* The policies MCC has do not fully address all Federal requirements. Further, MCC lacks written policies and procedures on classifying documents, giving access to classified cables, and maintaining a security incident log. MCC officials acknowledged that documented policies needed improvement. System limitations have also constrained MCC’s effectiveness to monitor and track staff who have taken required training.

CONCLUSION

Executive Order 13526 stressed the importance of safeguarding national security information. However, MCC’s classified national security information program does not fully comply with Executive Order 13526 or related regulations and directives. Although MCC derivatively classifies a small number of documents, it needs to improve its program policies and procedures, self-inspection program, declassification program, security education and training, and classification markings. New management in the security division has an opportunity to take meaningful corrective actions on these problems, some of which came up in OIG’s first evaluation and were not effectively resolved. Taking corrective actions to address the problems found in this review and deficiencies noted during OIG’s first evaluation, along with documenting key processes, will help provide greater assurance that documents are adequately classified, handled, and safeguarded.

RECOMMENDATION

***Recommendation 1.** We recommend that the Millennium Challenge Corporation's Domestic and International Security Division, in coordination with the Office of the General Counsel, implement a corrective action plan that addresses the Office of Inspector General's review results, to strengthen the agency's classified national security information program and achieve full compliance with Executive Order 13526 and Information Security Oversight Office regulations and directives.*

EVALUATION OF MANAGEMENT COMMENTS

We provided a draft of our report to MCC's Domestic and International Security Managing Director on September 12, 2016, for comment. MCC's Department of Administration and Finance provided comments in a memorandum dated September 21, 2016.

MCC agreed with our recommendation and described planned actions and completion dates to address it. All actions are to be completed by September 30, 2017. We therefore acknowledge MCC's management decision on recommendation 1.

MCC's comments are included in their entirety in appendix II.

SCOPE AND METHODOLOGY

Scope

We conducted this review following internally established OIG policies that govern the planning, conducting, and reporting of this work product. Those policies require that the review team be competent and independent, conduct its work using reasonable care, and follow established quality control procedures. The policies also require that we obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions in accordance with our review objectives. We believe that the evidence obtained provides that reasonable basis.

The review scope covered MCC's classified national security information activities since OIG's first evaluation.⁵ This included examining classified documents from board meetings held between December 10, 2013, and December 16, 2015, and reviewing evidence of training completed in 2014 and 2015. We conducted fieldwork from December 18, 2015, to September 1, 2016, at MCC's office in Washington, DC.

The review objectives were to (1) identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material at MCC; (2) assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered at MCC; and (3) determine whether MCC addressed recommendations OIG made in its previous report.

Methodology

We generally applied the methodology from the Department of Defense Inspector General's "A Standard User's Guide for Inspectors General Conducting Evaluations Under Public Law 111-258, the 'Reducing Over-Classification Act.'"

We interviewed officials from MCC's Domestic and International Security Division, Office of the General Counsel, and the Office of the Chief Information Officer about MCC's classified national security information activities.

We obtained an understanding of the process MCC uses to classify board meeting minutes and transcripts and of how it handles and safeguards classified Department of State cables. We also gained familiarity with how it records security incidents.

We tested all 18 classified board meeting transcripts and minutes from board meetings held December 10, 2013, to December 16, 2015, to determine whether they contained the appropriate classification markings and were classified at the appropriate level. To make this determination, we examined the reason for the classification to see if it seemed reasonable. In addition to the 18 documents, we reviewed select classified documents related to previous board meetings to obtain an understanding of how the classification process has changed over the years. The results of our testing cannot be extrapolated to the universe of classified documents.

⁵ "Evaluation of Millennium Challenge Corporation's Implementation of Executive Order 13526, Classified National Security Information" (M-000-15-001-S), December 18, 2014.

We assessed whether MCC's classified national security information program complied with Executive Order 13526 and ISOO regulations and directives for original classification authority, program management, security education and training, self-inspections, classification guide content, ISOO reporting, classification markings, and policies and procedures. This included comparing MCC's classified national security information policies with the requirements in the order and regulations.

We reviewed MCC's compliance with the security education and training requirements in the Executive order. This included a review of MCC's compliance with 2014 and 2015 training for individuals with original classification authority and the 2015 annual refresher training for all staff. This included observing MCC's SharePoint training site and obtaining staff training records.

We reviewed MCC's fiscal year 2015 "Agency Security Classification Management Program Data" report to ISOO and interviewed two individuals from ISOO about MCC's reporting.

We reviewed MCC's management decisions and final actions on the recommendations in OIG's first evaluation and assessed whether they effectively addressed the recommendations.

MANAGEMENT COMMENTS



MEMORANDUM

DATE: September 21, 2016

TO: Mark Norman
Acting Deputy Assistant Inspector General
Office of the Inspector General
United States Agency for International Development
Millennium Challenge Corporation

FROM: Jim Blades /s/
Acting Vice President, Contracts and Administration
Department of Administration and Finance
Millennium Challenge Corporation

Doug Fairfield /s/
Managing Director, Domestic and International Security
Department of Administration and Finance
Millennium Challenge Corporation

SUBJECT: MCC's Management Response to the Draft Report, *MCC's Implementation of Executive Order 13526, Classified National Security Information, Needs Strengthening*, dated September 12, 2016

Millennium Challenge Corporation (MCC) appreciates the opportunity to comment on the draft report on the Office of Inspector's review, *MCC's Implementation of Executive Order 13526, Classified National Security Information, Needs Strengthening*, dated September 12, 2016. MCC has found the review constructive for helping to bring MCC's classified national security program into compliance with the requirements of the Order and its implementing regulations and directives, and focusing the need to correct issues in specific areas. The formalization of written policy and procedures will greatly reduce compliance and performance issues arising from unplanned turnover of staff and greatly improve understanding of requirements and responsibilities.

Our Management Response to your recommendations follows.

OIG Recommendation 1: We recommend that the MCC's Domestic and International Security

Division, in coordination with the Office of the General Counsel, implement a corrective action plan that addresses the Office of Inspector General's review results, to strengthen the agency's classified national security information program and achieve full compliance with Executive Order 13526 and Information Security Oversight Office regulations and directives.

See the enclosed MCC Classified National Security Information Program Corrective Action Plan.

If you have any questions or require any additional information, please contact Doug Fairfield, Domestic & International Security Managing Director, at 202-521-3684 or FairfieldDH@mcc.gov; or Jude Koval, Director of Internal Controls and Audit Compliance (ICAC), at 202-521-7280 or KovalJG@mcc.gov.

CC: Donell Ries, Deputy Assistant Inspector General, OIG, USAID
Mark A. Spina, Director of Audits Division, OIG, USAID
Aleta Johnson, Administrative Assistant, OIG, USAID
William Barboza, Director, Domestic Physical and Personnel Security, DIS, A&F, MCC
Daren Wong, Director, Security Policy and Systems, DIS, A&F, MCC
Jim Blades, Acting Vice President, Administration and Contracts
Mahmoud Bah, Acting Vice President and Chief Financial Officer, A&F, MCC
Eric Redmond, Controller, Financial Management Division (FMD), A&F, MCC
Sarah E. Fandell, Vice President, General Counsel and Corporate Secretary, MCC
Thomas Hohenthauer, Deputy General Counsel, OGC, MCC
Laura Leussing, Assistant General Counsel, OGC, MCC
Jude Koval, Director of ICAC, FMD, A&F, MCC
Karla L. Chryar, Compliance Officer (Contractor), ICAC, FMD, A&F, MCC

Enclosure

1. Corrective Action Plan

Enclosure

**MILLENNIUM CHALLENGE CORPORATION
CLASSIFIED NATIONAL SECURITY INFORMATION (CNSI) PROGRAM
CORRECTIVE ACTION PLAN**

Program Policies and Procedures	
OIG Report Finding	MCC Corrective Actions
<p>MCC policies and procedures do not cover the following requirements:</p> <ul style="list-style-type: none"> • Trainings required for derivative classifiers and those with original classification authority at MCC, as well as provisions for suspension of original classification authority when training requirements are not met. • Responsibilities for tracking and monitoring employees' training compliance. • Provisions for MCC security clearance holders to challenge classification of documents if they believe it is improper, along with a statement that employees are protected from retribution if they make such challenges. • The need for the agency to conduct a fundamental classification guidance review at least once every 5 years. 	<p>MCC will issue a comprehensive CNSI Program policy to implement the requirements of Executive Order 13526, Code of Federal Regulations Part 2001 and other directives and guidance, including policies and procedures covering original classification, derivative classification, classification challenges, declassification and downgrading, safeguarding, self-inspections, participation in fundamental guidance reviews, security education and training, and management and oversight by September 30, 2017.</p> <ul style="list-style-type: none"> • Additional details on specific topic areas where there are findings in the OIG report are included in the subsequent sections of this corrective action plan.
<p>The MCC policy <i>Providing Private Sector Board Members and Plus Ones Access to Confidential Information</i> should be revised since in at least one instance, the Board Meeting transcript and minutes were classified at the Secret level.</p>	<p>MCC's policy <i>Providing Private Sector Board Members and Plus Ones Access to Confidential Information</i> will be updated to address access to classification information up to the Secret level by November 30, 2016.</p>

Self-Inspection Program and Reporting	
OIG Report Finding	MCC Corrective Actions
<ul style="list-style-type: none"> • MCC did not conduct a formal self-inspection in FY 2015 • MCC responses in the FY15 report submitted to ISOO contained errors and inconsistencies: <ul style="list-style-type: none"> ○ Inconsistent statements about how the self-inspection program is administered and how often it is conducted ○ Erroneous statement that training covered classification challenges ○ Inconsistent statement about how often classified actions take place 	<ul style="list-style-type: none"> • MCC submitted a report to ISOO providing results of its FY 2015 self-inspection. However, MCC did not follow its own procedures for drafting a detailed report to its senior agency official. MCC will conduct a formal report in accordance with its policies and procedures in FY 2016. • MCC will formally establish and periodically update coverage, frequency, and procedures and standards for evaluation of MCC CNSI Program self-inspections consistent with the requirements of Executive Order 13526 and 32 CFR 2001 Subpart F, including original classification, derivative classification, declassification, safeguarding, security violations, security education and training, and management and oversight by September 30, 2017. The first instance establishing coverage, frequency, and procedures and standards for evaluation will be completed by October 7, 2016 and will address the issues raised in the OIG report. <ul style="list-style-type: none"> ○ The instance will be applied to perform a self-inspection during the balance in October 2016 to contribute to MCC's FY 2016 self-inspection report to its senior agency official and the report due to the ISOO by November 15, 2016.

Declassification Program	
OIG Report Finding	MCC Corrective Actions
<ul style="list-style-type: none"> MCC does not have a declassification policy but plans to create one covering review procedures. 	<ul style="list-style-type: none"> MCC's declassification program policies and procedures will be included in MCC's CNSI Program policy to be completed by September 30, 2017.

Security Education and Training	
OIG Report Finding	MCC Corrective Actions
<ul style="list-style-type: none"> Not all those at MCC with original classification authority took the required training. MCC cannot determine whether each person requiring annual refresher training had taken the training. The agency had no centralized mechanism for tracking the exceptions. 	<ul style="list-style-type: none"> MCC will draft procedures and implement them for mandatory original classification authority training, derivative classifier training, and CNSI refresher training, consistent with the requirements of Executive Order 13526 and 32 CFR 2001 Subpart G by November 30, 2016. The procedures will include DIS' responsibilities to: <ul style="list-style-type: none"> Maintain records of completion of mandatory CNSI program training for each individual holding a MCC security clearance or interim security clearance and approved waivers of mandatory training requirements. Keep original classification authorities and derivative classifiers informed of the requirements for mandatory trainings to establish and maintain their authority to classify documents, and notify them of the schedule of training events that will allow them to satisfy their mandatory training requirements. Inform holders of MCC security and interim security clearances of the training requirements and notify them of the schedule of training events that will allow them to satisfy their mandatory trainings. <p>The procedures will be incorporated into MCC's CNSI Program policy to be completed by September 30, 2017.</p>

Classification Markings	
OIG Report Finding	MCC Corrective Actions
<ul style="list-style-type: none"> • It was not always clear how the declassification date was established • Not all meeting minutes contained approval signatures • Only one transcript had a declassification date 	<ul style="list-style-type: none"> • MCC's CNSI Program policy will include guidelines for proper marking of classified documents and procedures for classifying Board Meeting transcripts and minutes. The policy will be completed by September 30, 2017.

Documentation of Internal Controls for Managing Classified Information	
OIG Report Finding	MCC Corrective Actions
<ul style="list-style-type: none"> • MCC needs written procedures for recording and classifying meeting transcripts and minutes • MCC needs written procedures for giving access to State Department cables • MCC needs procedures for maintaining and updating its security incident log 	<ul style="list-style-type: none"> • The following written procedures will be included in MCC's CNSI Program policy to be completed by September 30, 2017. <ul style="list-style-type: none"> ○ Recording and classifying Board Meeting transcripts and minutes ○ Access, use and disposal of hard copies of Department of State cables ○ Recording and reporting of security incidents

Insufficient MCC Actions on Prior OIG Recommendations	
OIG Report Finding	MCC Corrective Actions
<p>Recommendation 1</p> <ul style="list-style-type: none"> • MCC is not verifying compliance with marking requirements in its annual self-inspection reports. 	<ul style="list-style-type: none"> • Action on this issue is addressed in Self-Inspection Program and Reporting.
<p>Recommendation 2</p> <ul style="list-style-type: none"> • MCC needs to assure original classification authorities complete their required training or obtain waivers. MCC must take actions to prevent training lapses. 	<ul style="list-style-type: none"> • Action on this issue is addressed in Security Education and Training.
<p>Recommendation 3</p> <ul style="list-style-type: none"> • Establish formal guidance requiring documentation of completion of Executive Order 13526 training requirements for all employees, including original classification authorities. 	<ul style="list-style-type: none"> • Action on this issue is addressed in Security Education and Training.

**U.S. Agency for International Development
Office of Inspector General**

1099 14th Street, NW, Suite 825

Washington, DC 20005

Tel: 202-712-1150

Fax: 202-216-3047

<https://oig.usaid.gov>

Review Task No. MM100616