Office of Inspector General

December 18, 2014
Mr. William Barboza
Director of Security and Office Services
Millennium Challenge Corporation
875 15th Street, NW
Washington, DC 20005

Dear Mr. Barboza:

This letter transmits the Office of Inspector General's (OIG's) *Evaluation of Millennium Challenge Corporation's Implementation of Executive Order 13526, Classified National Security Information* (M-000-15-001-S). In finalizing the report, we considered your written comments on our draft report and included those comments in their entirety in Appendix II.

The report contains four recommendations. We acknowledge MCC's management decisions on all of them.

We appreciate the cooperation and courtesy extended to our staff during this audit.

Sincerely,

/s/

Melinda Dempsey
Deputy Assistant Inspector General for Audit
Millennium Challenge Corporation

cc: Matt Bohn, Vice President, Department of Administration and Finance and Chief Financial Officer
Karla Chryar, Compliance Officer
Robert Fry, OIG

SUMMARY

On December 29, 2009, President Barack Obama issued Executive Order (EO) 13526, "Classified National Security Information," which outlined how national security information should be classified and protected. He explained the rationale behind the order in a memorandum released several months earlier.

> While the Government must be able to prevent the public disclosure of information where such disclosure would compromise the privacy of American citizens, national security or other legitimate interests, a democratic government accountable to the people must be as transparent as possible and must not withhold information for self-serving reasons or simply to avoid embarrassment.[1]

EO 13526 states that information may be classified by an "original classification authority" (OCA), an agency official with the delegated authority to classify information. The OCA can classify information at three levels, listed below.

1. Top secret shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to national security.

2. Secret shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to national security.

3. Confidential shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to national security.

Information may be classified as original or "derivative." EO 13526 defines original classification as an initial determination that information must be protected from unauthorized disclosure in the interest of national security. It defines derivative classification as incorporating, paraphrasing, restating, or generating information that is already classified and then transferring the original classification markings to the new material.

Information may be derivatively classified from original documents or by using a classification guide. Employees who apply derivative classification markings must be trained to apply the principles of EO 13526 before classifying information and at least once every 2 years afterward.

Three Millennium Challenge Corporation (MCC) officials were designated as OCAs to classify documents up to the secret level: the chief executive officer (CEO); the vice president/general counsel, who also serves as corporate secretary; and the vice president of the Department of Compact Operations. According to MCC, these officials also have the authority to derivatively classify documents.

[1] http://www.whitehouse.gov/the_press_office/Presidential-Memorandum-Classified-Information-and-Controlled-Unclassified-Information/.

Minutes of MCC's board of directors[2] meetings are the only documents that MCC derivatively classifies. MCC officials said the board used a device accredited to secret level to record the meetings, which were held at the State Department. MCC then used the recorded discussions to document, classify, mark, and label the minutes. Board members approve them at the beginning of the following meeting.

MCC had derivatively classified as confidential minutes from eight of nine quarterly board meetings since September 2011. In the one exception, the minutes were marked as sensitive but unclassified.

OIG conducted this evaluation to fulfill requirements in the Reducing Over-Classification Act (Public Law 111-258), enacted on October 7, 2010. This called for inspectors general to assess whether applicable classification policies, procedures, rules, and regulations had been adopted, followed, and managed, and to identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material.

OIG found that MCC generally adopted the classification policies, procedures, rules, and regulations prescribed by EO 13526. We did not find evidence that material had been misclassified persistently or overclassified. MCC properly classified the minutes we reviewed.

However, MCC did not mark the board meeting minutes correctly (page 3), and MCC officials did not complete required training (page 3). If not corrected, these practices could lead to material being misclassified. In addition, MCC's policy on storing the minutes is out of date (page 4).

To address these concerns, OIG recommends that MCC's Director of Security and Office Services:

1. Verify that the board meeting minutes from September 2011 to September 2013 are marked properly and provide the results of the verification to OIG, (2) include instructions on how to correctly mark derivative classification documents in MCC mandatory training courses, and (3) verify compliance with marking requirements in annual self-inspection reports (page 3).

2. Document that all OCAs have completed required training or obtained waivers (page 4).

3. Establish formal guidance that requires documentation of completion of EO 13526 training requirements for all employees, including OCAs (page 4).

4. Update the *Procedures for MCC Private Sector Board Members and Plus Ones for Storing Confidential Information* in GSA-approved safes or submit alternative measures to the Information Security Oversight Office, as required (page 5).

Detailed results of our evaluation appear in the following section. The scope and methodology appear in Appendix I. Our evaluation of management comments is on page 6, and the full text of management comments is in Appendix II.

[2] The board consists of the Secretary of State (chair), the Secretary of Treasury (vice chair), the U.S. Trade Representative, the USAID Administrator, the CEO of MCC, and four members of the private sector appointed by the President.

EVALUATION RESULTS

MCC Incorrectly Marked Classified Documents

Both the MCC *Classification Guide*, dated August 4, 2011, and the Information Security Oversight Office marking booklet, dated January 1, 2012, require that classified documents are clearly marked in a specific manner. Derivatively classified documents must include a classification authority section or "block," that identifies the person classifying the document, sources of classified information, or classification guide, and the date or event for declassification. The guide also states, "A new requirement of the executive order is that derivative classifiers be identified by name and position. This should be indicated after the 'derived from' line."

MCC did not follow the marking requirements for derivatively classifying MCC board meeting minutes at the confidential level. We reviewed all confidential minutes classified and marked after the guide was issued in August 2011. Although they were classified properly, none of the documents included the name of the person who classified them, a "derived from" line, or a date. One document did not include the classification authority block at all.

MCC incorrectly marked the minutes because the principal classifier was not taught how to mark documents that needed derivative classification. MCC's initial training and annual security refresher training did not include marking requirements for derivative classification. Instead, both training courses only covered requirements for marking originally classified documents.

Complete classification markings are critical for protecting national security information and complying with security regulations. Without the name of the original classifier, a "derived from" list of sources, or reference to the classification guide, classifiers might not know how to classify future documents properly. Not listing declassification dates may result in documents remaining classified for longer than necessary and needlessly limiting access to information.

To address these concerns, we make the following recommendation.

> ***Recommendation 1.*** *We recommend that the Millennium Challenge Corporation's Director of Security (1) verify that the board meeting minutes from September 2011 to September 2013 are marked properly and provide the results of the verification to OIG, (2) include instructions on how to correctly mark derivative classification documents in Millennium Challenge Corporation mandatory training courses, and (3) verify compliance with marking requirements in annual self-inspection reports.*

MCC Officials Did Not Complete Required Training

EO 13526 required annual security clearance training and recertification for all federal employees who have a security clearance. In addition, it provided specific training requirements for employees designated as OCAs, as well as those who were derivative classifiers.

OCAs must receive training on proper classification, particularly to avoid overclassifying and incorrectly declassifying information. Training must include instructions on how to protect classified information properly and what sanctions might be brought against anyone who does not classify information properly or protect classified material from unauthorized disclosure. Employees who did not receive the required training at least once a year would have their classification authority suspended by the agency head. However, the head could grant a waiver.

Derivative classifiers had similar, but slightly different requirements. These employees must receive instructions on how to apply derivative application principles properly at least once every 2 years. They also are subject to the same sanctions if they do not complete the training.

MCC conducted training for new employees and annual security training for all employees. However, MCC officials could not provide documents showing that any of the three officials designated as OCAs had completed specialized training or received waivers.

MCC monitored completion of new employee and annual refresher security training through records kept in its security database. The associate director of security prepared a list of employees who did not complete training by the end of the calendar year and sent it to the director to follow up with the employees and their supervisors. However, officials said the database did not include OCA training data.

MCC did not train the officials properly because the *Classification Guide* did not address the training requirements or waivers that were required for the specialized security training.

By not providing proper training, MCC does not comply with EO 13526 and runs the risk of improperly classifying data. Further, the OCAs may not know what their security responsibilities entail and may classify information without proper authority. To address these concerns, we make the following recommendations.

> ***Recommendation 2.*** *We recommend that the Millennium Challenge Corporation's Director of Security document that all original classification authorities have completed required training or obtained waivers.*
>
> ***Recommendation 3.*** *We recommend that the Millennium Challenge Corporation's Director of Security establish formal guidance that requires documentation of completion of Executive Order 13526 training requirements for all employees, including original classification authorities.*

MCC Document Storage Procedures Were Out of Date

Title 32 of the Code of Federal Regulations (CFR), Section 2001.43, published in July 2010, lists procedures for storing top secret, secret, and confidential information. According to that, agencies could use various types of containers that did not have to be approved by the General Services Administration (GSA) until October 2012. After that date, agencies had to either use containers specifically approved by GSA or present alternative procedures to the director of the Information Security Oversight Office, the organization responsible for ensuring that the U.S. Government protects and provides proper access to information.

MCC's rules for how board members were supposed to store classified information did not comply fully with the CFR. *Procedures for MCC Private Sector Board Members and Plus Ones for Storing Confidential Information*, issued in 2009, allowed them to use a reasonably secure cabinet or lockbox. However, MCC did not amend those rules after October 2012 when it should have either switched to GSA-approved containers or presented alternative procedures to the Information Security Oversight Office.

MCC officials could not explain why the procedures had not been updated. By not updating its procedures, MCC does not comply with current regulations. To address this concern, we make the following recommendation.

> ***Recommendation 4.*** *We recommend that the Millennium Challenge Corporation's Director of Security update the* Procedures for MCC Private Sector Board Members and Plus Ones for Storing Confidential Information *in GSA-approved safes or submit alternative measures to the Information Security Oversight Office, as required.*

EVALUATION OF MANAGEMENT COMMENTS

MCC agreed with all four recommendations. In addition to providing the management comments in Appendix II, MCC officials clarified their comments in subsequent conversations with OIG.

Recommendation 1. MCC agreed to verify that the board meeting minutes from September 2011 to September 2013 were marked properly and provide the results of the verification to OIG by December 31, 2014. MCC also agreed to include instructions on how to mark derivative classification documents correctly in MCC mandatory training courses, and it plans to provide specific slides and questions in a quiz to verify that employees understand what to do. MCC agreed to verify compliance with marking requirements in annual self-inspection reports.

OIG acknowledges MCC's management decision. Final action will occur when MCC gives OIG the results of its verification of the board meeting minutes from September 2011 to September 2013.

Recommendation 2. MCC agreed with the recommendation and will provide required training to its three OCAs by December 31, 2014. OIG acknowledges MCC's management decision. Final action will occur when MCC provides OIG with documentation that the training was completed.

Recommendation 3. MCC agreed to establish formal guidance by March 31, 2015, that requires documentation of completion of EO 13526 training requirements for all employees, including OCAs. MCC will document completion of training on its Sharepoint site. OIG acknowledges MCC's management decision. Final action will occur when MCC provides OIG with the guidance.

Recommendation 4. MCC agreed to review and update *Procedures for MCC Private Sector Board Members and Plus Ones for Storing Confidential Information* by March 31, 2015. OIG acknowledges MCC's management decision. Final action will occur when MCC provides OIG with the updated procedures document.

SCOPE AND METHODOLOGY

Scope

We conducted this performance evaluation in response to the Reducing Over-Classification Act, dated October 7, 2010. We conducted our evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation issued in 2012. These standards require that we plan and perform our evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions in accordance with the evaluation objective. We believe that the evidence obtained provides that reasonable basis.

Our objectives were to determine whether applicable classification policies, procedures, rules, and regulations had been adopted, followed, and administered effectively within MCC, and to identify policies, procedures, rules, regulations, or management practices that might be contributing to persistent misclassification of material within MCC.

MCC derivatively classified only its board meeting minutes and no other documents. The board meets four times a year. Our scope covered board meeting minutes from September 2011 to September 2013.[3] This was OIG's first evaluation of MCC's classification procedures. We conducted our fieldwork in Washington, D.C., from January 16, 2014, to February 21, 2014.

Methodology

To answer our evaluation objectives, we reviewed MCC's classified information policies, procedures, rules, regulations, and management practices.

We interviewed select MCC officials with original and derivative classification authority to gain an understanding of their roles and responsibilities regarding document classification and MCC's document classification process. In addition, we interviewed MCC officials to discuss any discrepancies identified during our evaluation fieldwork. We followed up with MCC officials and the Information Security Oversight Office to discuss discrepancies identified during fieldwork.

We reviewed the internal controls related to the classification process, training, and other miscellaneous topics related to security at MCC. In particular, we discussed classification and markings procedures with MCC officials, and reviewed classified documents and training records to assess their compliance with the procedures.

Because minutes from only nine MCC board meetings had been prepared since MCC's *Classification Guide* was published in August 2011, we judgmentally selected and reviewed those nine.[4] Our results are therefore limited to them. We reviewed the minutes to see whether they were classified, marked, and labeled according to the guide and EO 13526. In addition, we reviewed training documents for select MCC personnel and self-inspection reports.

[3] The September 2013 meeting minutes were the most recently approved at the time of our fieldwork.
[4] Minutes for one of the meetings were marked as sensitive but unclassified.

MANAGEMENT COMMENTS

October 31, 2014

Ms. Melinda Dempsey
Deputy Assistant Inspector General for Audit
Millennium Challenge Corporation
1401 H Street, NW (Suite 770)
Washington, DC 20005

Dear Ms. Dempsey:

This letter responds to your October 10, 2014 letter which transmitted the Office of the Inspector General's draft report on "Evaluation of Millennium Challenge Corporation's Implementation of Executive Order 13526, Classified National Security Information" (M-000-15-00X-P). This response reflects MCC's position regarding each of the four recommendations included in your October 10, 2014 letter, as follows:

Recommendation 1. We recommend that the MCC's Director of Security (1) verify that the board meeting minutes from September 2011 to September 2013 are marked properly and provide the results of the verification to OIG, (2) include instructions on how to correctly mark derivative classification documents in MCC mandatory training courses, and (3) verify compliance with marking requirements in annual self-inspection reports.

MCC Response to Recommendation 1: Before/by COB on Friday, October 31, 2014, MCC's Director of Security will (1) verify that the board meeting minutes from September 2011 to September 2013 are marked properly and provide the results of the verification to OIG; (2) include the following instructions on how to correctly mark derivative classification documents in MCC mandatory training courses:

5 FAM 480 CLASSIFYING AND DECLASSIFYING NATIONAL SECURITY INFORMATION—E.O. 13526
(CT: IM-149; 04-24-2014)
5 FAM 482.3 Derivative Classification Authority
(CT: IM-117; 06-16-2011)

a. Using the Department's Classification Guide. As explained in Part 2 of E.O. 13526, derivative classification is permitted where classification decisions are made in accordance with the instructions contained in an agency classification guide. Department's Classification Guide, which may be found on CLASSNET at http://a.m.state.class/sites/gis/ips/default.aspx, provides detailed guidance on the

proper classification of the types of information most frequently classified by the Department. Use of the Classification Guide is the preferred method of classification and is aimed at ensuring uniformity and conformity with government-wide classification standards. While classifying information based on the Classification Guide is a form of derivative classification, it is different from restating or otherwise using information that is already classified (see 5 FAM 482.3 paragraph b, below). As with the person who reproduces, extracts, or summarizes information that is already classified, the person who applies classification markings based on or as directed by a classification guide need not possess original classification authority. However, it is essential that the material being classified and the level and duration of classification fit within the provisions for classification set forth in the Classification Guide, including the general prohibition against derivatively classifying information for more than twenty-five years on the basis of a classification guide except for information that should clearly and demonstrably be expected to reveal the identity of a confidential human source, a human intelligence source, or key design concepts of weapons of mass destruction, and specific information incorporated into classification guides in accordance with section 2.2(e) of E.O. 13526.The Order also requires that derivative classifiers be identified by name and position on the classified information and that they receive training at least once every two years or they will lose their derivative classification authority.

b. Using Information That Is Already Classified. Another form of derivative classification is the incorporating, paraphrasing, restating, or generating in a new form information that is already classified and then marking the newly developed material consistent with the classified markings that apply to the source information. Although persons who reproduce, extract, or summarize classified information need not possess original classification authority, they must observe and respect the original classification decisions and carry forward to any newly created documents the pertinent classification markings (see 5 FAM 482.11, below). When already classified information is incompletely or improperly marked (e.g., the declassification date is greater than 25 years, no reason is stated, etc.) derivative classifiers should remedy the error. If classifiers have a question when remedying the error, they should ask the first OCA in their supervisory chain or email classification@state.gov or, if classified information is contained, to classification@state.sgov.gov. All sources for derivatively classified information must be identified; when multiple sources are noted, a list of all sources must be included with the new classified document.

and (3) verify compliance with marking requirements in annual self-inspection reports, as follows: In the CY2014 and all CYs going forward, Annual Security Clearance Revalidation Training and Recertification Quiz, the training slides and accompanying quiz will include derivative marking training and verification knowledge responses.

Recommendation 2. We recommend that the MCC's Director of Security document that all Original Classification Authorities have completed required training or obtained waivers.

MCC Response to Recommendation 2: Please see attached October 14, 2014 e-mail from Joyce B. Lanham to MCC's three OCAs – Dana Hyde, Tom Hohenthaner and Kamran Khan – advising them of mandatory annual training for OCAs delegated by the Secretary of State. A package of all of the documents listed in her e-mail to each of the individuals named above as well as the Director of Security and the Associate Director Ms. Lanham will register and complete the on-line training, FSI course description of PK323 – Classified and Sensitive But Unclassified Information: Identifying & Marking, in order to assist MCC's three OCAs complete their training before/by December 31, 2014.

Recommendation 3. We recommend that the Millennium Challenge Corporation's Director of Security establish formal guidance that requires documentation of completion of Executive Order 13526 training requirements for all employees, including Original Classification Authorities.

MCC Response to Recommendation 3: Each Annual Security Clearance Revalidation and Recertification Quiz is documented on Security's Sharepoint site at: http://intranet.mcc.gov/department/AF-Security/SecurityQuiz/SitePages/Home.aspx which is required of all MCC FTEs and the three OCAs will be required to complete PK323–Classified and Sensitive But Unclassified Information: Identifying & Marking on an annual basis.

Recommendation 4. We recommend that the MCC's Director of Security update the Procedures for MCC Private Sector Board Members and Plus Ones for Storing Confidential Information *in GSA-approved safes or submit alternative measures to the Information Security Oversight Office, as required.*

MCC Response to Recommendation 4:
The 2009 Storing Confidential Information policy will be reviewed and updated to reflect alternate procedures Board Members and Plus Ones shall use to receive and review confidential information.

Sincerely yours,

/s/

William J. Barboza
Director of Security & Office Services

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