Office of Inspector General
for the Millennium Challenge Corporation

June 1, 2011

Ms. Victoria B. Wassmer
Vice President of Department of Administration and Finance
Millennium Challenge Corporation
875 Fifteenth Street, N.W.
Washington, DC 20005

Dear Ms. Wassmer:

This letter transmits the Office of Inspector General's final report on the *Survey of the Millennium Challenge Corporation's Implementation of Selected Controls Over Personal Digital Assistants* (M-000-11-007-S). In finalizing this report, we considered your written comments on our draft report and included those comments in their entirety in Appendix II of this report.

Although this is not an audit report, it contains four recommendations to strengthen the Millennium Challenge Corporation's controls over its personal digital assistants. We agree with MCC's management decisions for Recommendations 1, 2, 3, and 4.

I appreciate the cooperation and courtesy extended to my staff during this audit.

Sincerely,

/s/

Alvin A. Brown
Assistant Inspector General
Millennium Challenge Corporation

cc: Mark Sandy, Managing Director, Administration and Finance
Dennis Laurer, Chief Information Officer
Arlene McDonald, Compliance Officer

Millennium Challenge Corporation
1401 H Street, NW
Suite 770
Washington, DC 20005
www.usaid.govoig

SUMMARY

A personal digital assistant (PDA) is a mobile device that may be used for voice calls, text messages, data storage, accessing the Internet, sending/receiving e-mail, and performing other tasks such as calculations. Nonetheless, PDAs have a variety of risks, including improper personal use and unauthorized access.

The Millennium Challenge Corporation (MCC) has an average of 315 PDA users, and budgeted $480,000 in fiscal year 2011 for PDA services. This survey was initiated to determine whether MCC implemented selected controls to reduce the risks to its PDAs. For this survey, selected controls were (1) approval for staff to receive PDAs, (2) reviews of PDA charges, (3) collections for unauthorized use of PDAs, and (4) selected security controls.

This survey found that MCC implemented the following controls over its PDAs:

- Collected money from its PDA users for unauthorized charges reported to the Chief Information Officer.
- Adopted the Department of Defense checklist as the baseline for securing its BlackBerrys.
- Documented its BlackBerry configuration security policy.
- Prepared a *Policy on Personal Digital Assistants* (November 26, 2008) to inform employees about the laws, regulations, and policies governing the issuance and use of MCC-owned PDAs.
- Configured the server for the PDAs to perform the following functions:
  - Encrypt the disks
  - Require an 8-character alphanumeric password
  - Lock after 15 minutes of inactivity and require that the user reenter the PDA's password to unlock the device
  - Block the installation of third-party software
  - Prevent users from disabling the password requirement
  - Prevent outgoing calls when the device is locked

Nonetheless, MCC did not (1) prepare procedures for reviewing PDA bills (pages 3–4), (2) consistently document PDA approvals for staff at the level of program officer and above and for full-time personal service contractors (PSCs) (page 4), or (3) consistently prepare justifications for issuance of PDAs (pages 5–6). To correct these control weaknesses, this report recommends that MCC:

1. Develop procedures to review PDA bills (page 4)
2. Document and implement procedures for program officers and above and full-time personal service contractors to receive PDAs (page 5)
3. Revise MCC's PDA policy to reflect the current management position regarding the issuance of PDAs to staff who are program officers and above and full-time PSCs (page 5)
4. Prepare and implement documented procedures to define what information is required to justify the need for staff below the program officer level, contractors, and intermittent PSCs to receive a PDA (page 6)

Detailed results of this survey appear in the following section. Appendix I contains the scope and methodology. MCC provided comments on the draft report, which are included in their entirety in Appendix II. OIG agrees with MCC's management decisions on all four recommendations (page 7).

SURVEY FINDINGS

Procedures Not Prepared for Reviews of Personal Digital Assistant Bills

MCC's *Policy on Personal Digital Assistants* (November 26, 2008), section 5.2, states:

> MCC employees will reimburse MCC for all personal calls that result in an increased cost to MCC. Department vice presidents will ensure that monthly PDA bills are reviewed and must report any unauthorized PDA use to the CIO [Chief Information Officer] by the 20th of every month.

In addition, the U.S. Government Accountability Office's[1] *Standards for Internal Control in the Federal Government* (November 1999) states that "[i]nternal control and all transactions and other significant events need to be clearly documented, and the documentation should be readily available for examination." Further, "[a]ll documentation and records should be properly managed and maintained."

However, MCC did not maintain documentation of its reviews of PDA bills. MCC officials acknowledged that MCC does not have procedures for implementing its PDA policy. Specifically, MCC does not have procedures that explain to MCC staff what documentation must be maintained for reviews of PDA bills or that require staff to certify that the bills were reviewed. In addition, MCC does not have procedures describing how MCC staff should conduct their reviews, including which items to focus on (e.g., roaming charges, excessive airtime minutes). Finally, although one department established a $200 threshold, MCC did not establish corporation-wide thresholds for when to conduct a detailed review of an individual's charges.

As a result, MCC did not have assurance that it was reimbursed for unauthorized staff calls. For example, Table 1 shows that from August through December 2010 there were 342[2] instances (totaling more than $124,000)[3] in which individual PDA users' charges exceeded $100.

Table 1. Total Individuals' Monthly Charges Over $100 (August–December 2010)[4]

Range of Monthly Charges	No.	Amount
$101–$200	148	$20,985
$201–$299	60	$15,288
$300–$500	55	$20,529
Over $500	79	$67,605
Total	**342**	**$124,407**

In addition, the individual responsible for administratively approving the PDA bill for payment had no assurance that the amounts approved for payment were correct, as

[1] Formerly called the General Accounting Office.
[2] Unaudited.
[3] Unaudited.
[4] Unaudited; Source: OIG analysis of MCC' data on PDA charges.

required by the delegation of authority from the cognizant contracting officer. For the first 11 months of fiscal year 2010, approved payments amounted to more than $425,000.[5] Finally, it is imperative that MCC implement controls over areas such as this, which the public can perceive as Government abuse. Therefore, OIG makes the following recommendation.

> ***Recommendation 1.*** *We recommend that the Millennium Challenge Corporation's Chief Information Officer develop procedures for reviews of its personal digital assistants bills, including—*
>
> - *Requirements to maintain documentation that bills were reviewed, including certifications from those responsible for reviewing the bills.*
> - *A description of how the reviews should be conducted, including what items to focus on and organization-wide thresholds for when to conduct detailed reviews of an individual's charges.*

Required Approvals Not Consistently Documented for Issuance of PDAs

According to MCC's *Policy on Personal Digital Assistants*, section 5.1:

> Employees at the level of program officers and above and full-time personal services contractors (PSC) may receive a PDA. However, the employee's supervising managing director should make an individualized decision as to whether or not an employee should be issued a PDA.

MCC did not consistently document PDA approvals for staff at the level of program officer and above and full-time PSCs. Specifically, MCC staff who already had a BlackBerry before BlackBerrys were replaced or upgraded from December 2008 through March 2009 were given a new one without receiving approval from their supervisor. In addition, after the refresh, those who were directors or above received a PDA upon request, whereas an e-mail approval was required only for those below the director level.

This weakness occurred primarily because MCC did not document and implement procedures describing the documentation of approvals required for employees at the level of program officers and above and full-time PSCs. Moreover, although MCC policy requires those individuals to have supervisory approvals, MCC management's views may have changed concerning who should receive a PDA. Specifically, although a definitive position has not been reached, MCC management seems to believe that all program officers and above and full-time PSCs need to be issued a PDA as part of the standard equipment, such as computers and telephones. Thus, MCC's PDA policy may be outdated.

Because MCC staff have not received approvals, MCC has no assurance that staff who have PDAs need them to conduct MCC business. Therefore, OIG makes the following recommendations.

[5] Unaudited.

Recommendation 2. *We recommend that the Millennium Challenge Corporation's Chief Information Officer document and implement procedures (a) describing the required documentation that supervisors must submit for program officers and above and full-time personal service contractors to receive personal digital assistants and (b) requiring supervisors to periodically recertify (in a predefined timeframe) staffs' continued need for personal digital assistants.*

Recommendation 3. *We recommend that the Millennium Challenge Corporation's Chief Information Officer review and revise the Millennium Challenge Corporation's* Policy on Personal Digital Assistants *to reflect the Corporation's current management position regarding the issuance of personal digital assistants to staff who are program officers and above and full-time personal service contractors.*

Required Justifications Not Consistently Prepared for Issuance of PDAs

According to MCC's *Policy on Personal Digital Assistants*, section 5.1, employees at the level of program officers and above and full-time PSCs may receive a PDA. However, the policy further states that—

- Other MCC employees may receive PDAs if the employee's departmental vice president submits a written justification to the CIO.
- On-site independent contractors may be issued PDAs if their contracting officer's technical representative submits a written justification through their department's vice president. The vice president will endorse the request and the CIO will review the request.
- Intermittent PSCs require a waiver from the department vice president to receive a PDA.

All 10 BlackBerry users sampled had written waivers on file provided through their department vice presidents to the CIO. However, five of the waivers did not include a justification for providing those individuals with a PDA. Instead, those five waivers only cited sections from MCC PDA policy regarding the use of BlackBerrys and which employees could receive waivers. Further, two of the five waivers included handwritten names that had been added after the waivers were digitally signed. Thus, for the two it was not clear whether and when those users had gone through the required waiver process.

This problem occurred because MCC did not have procedures to define the information required to justify the need for a PDA. As a result, MCC did not have assurance that staff below the program officer level, contractors, and intermittent PSCs who have been issued PDAs need them to conduct official MCC business.

Since the time those justifications were prepared, MCC has developed an automated form that must be used to prepare waivers. The form allows only one name to be

entered, and the justification field cannot be blank. Nonetheless, as MCC officials acknowledged, MCC should periodically recertify whether all users continue to need a PDA. Therefore, OIG makes the following recommendation.

Recommendation 4. *We recommend that the Millennium Challenge Corporation's Chief Information Officer prepare and implement documented procedures to (a) define what information is required to justify the need for a personal digital assistant for staff below the program officer level, contractors, and intermittent personal service contractors and (b) require supervisors to periodically recertify (in a predefined timeframe) staffs' continued need for personal digital assistants.*

Evaluation of Management Comments

The Millennium Challenge Corporation provided written comments to the draft report that are included in their entirety in Appendix II. MCC agreed to take corrective action on all four recommendations in the draft report.

For Recommendation 1, MCC agreed to develop a procedure for the monthly review of PDA bills by April 1, 2012. OIG agrees with MCC's management decision.

For Recommendation 2, MCC agreed to develop guidelines consistent with MCC's PDA policy to outline the requirements for staff to receive PDAs. In addition, MCC agreed to prepare procedures requiring a documented business case for all staff who require PDAs and a semiannual recertification to document the continued need for PDAs. MCC will complete the guidelines and procedures by April 1, 2012. OIG agrees with MCC's management decision.

For Recommendation 3, MCC agreed to develop an information technology project risk management policy by April 8, 2011. OIG agrees with MCC's management decision.

For Recommendation 4, MCC agreed to update the Contracts Operating Manual to include procedures for incorporating risk management and earned value management in contracting actions, when required. MCC plans to take final corrective action by March 31, 2011. OIG agrees with MCC's management decision.

Scope and Methodology

Scope

OIG conducted this survey of the MCC's implementation of selected controls for its PDAs in accordance with *Government Auditing Standards*, except that OIG did not—

- Research and identify legal and regulatory requirements related to this survey objective.
- Assess audit risk.
- Perform a risk assessment via a team discussion to determine the likelihood that noncompliance resulting from illegal acts and fraud could have a significant impact on this survey objective.[6]
- Identify current OIG/Investigations cases or information related to the subject.
- Coordinate with other auditors.
- Perform specific tests for illegal acts, fraud, and abuse.

This survey was performed in Washington, DC, from February 3 through March 23, 2011. To answer our survey objective, we interviewed MCC officials and contractors responsible for PDAs. In addition, we reviewed contracting actions, MCC policies, waivers given to PDA users, and MCC's report on reimbursements for unauthorized PDA charges. We also analyzed PDA charges from August through December 2010 and user roles on the BlackBerry Enterprise Server. For this survey, we focused on the following selected controls: (1) approval for employees to receive PDAs, (2) reviews of PDA charges, (3) collections for unauthorized use, and (4) selected security controls.

Methodology

To answer the survey objective, using MCC's *Policy on Personal Digital Assistants* (November 26, 2008), OIG (1) reviewed approvals for MCC staff to receive PDAs, (2) assessed MCC's reviews of PDA charges, and (3) assessed collections for unauthorized use. OIG also evaluated selected security controls over PDAs based on MCC's *Information Systems Security Policy* (May 4, 2010). Specifically, OIG determined whether—

- A judgmental sample of MCC employees at or above the program officer level and full-time personal services contractors received approval from their respective supervisor managing director to receive PDAs. Specifically, we used a random number generator to select 10 (4 percent) of the 249 PDA users in this category, as shown in MCC's PDA inventory. We selected a relatively small percentage of the population because, in our opinion, those individuals are more likely need PDAs for business.

- Departmental vice presidents submitted a written justification to the Chief Information Officer for a judgmental sample of MCC employees below the program officer level, part-time personal services contractors, and on-site independent contractors to be

[6] No instances of illegal acts were identified during this survey.

issued PDAs. We used a random number generator to select 10 (15 percent) of the 65 PDA users in this category, as shown in MCC's PDA inventory. We selected a relatively large percentage of the population because, in our opinion, those individuals are less likely to need PDAs for business.

- Departmental vice presidents ensured that monthly PDA bills were reviewed and that unauthorized PDA use was reported the Chief Information Officer by the 20th of the month.

- MCC collected costs associated with unauthorized use of PDAs.

- MCC configured its PDAs in accordance with selected security requirements.

Management Comments

May 10, 2011

MEMORANDUM TO: **Alvin A. Brown**
Assistant Inspector General for the Millennium Challenge Corporation

FROM: **Dennis Lauer /s/**
Chief Information Officer (CIO)
Millennium Challenge Corporation (MCC)

SUBJECT: **MCC Comments on the Survey of the Millennium Challenge Corporation's Implementation of Selected Controls Over Personal Digital Assistants (M-000-11-00X-S).**

The Millennium Challenge Corporation (MCC) appreciates the opportunity to comment on the survey of the MCC's Implementation of Selected Controls over Personal Digital Assistants (PDAs). This memorandum serves as Management Decision for the four recommendations resulting from this survey.

MCC concurs with the four PDA survey recommendations and the two supplemental PDA survey recommendations. Considering that MCC has only operated for seven years, there has already been significant progress in establishing controls and governance over the PDA program, including:

1. MCC developed a Personal Data Assistant (PDA) Policy;

2. MCC has a monthly bill/usage review process;

3. Unlike many USG agencies, MCC has implemented Federal Desktop Core Configuration (FDCC) compliant security controls on all mobile devices;

4. MCC has initiated a review of the PDA policy to account for the recommendations in this survey; and

5. Between 2008 - 2011, MCC reduced the annual cost of PDAs by 25% and has set a goal to reduce the cost of PDAs by another 25% in the next year.

MCC's Management Response to your recommendations follows:

Recommendation No. 1: We recommend that the Millennium Challenge Corporation's Chief Information Officer develop procedures for reviews of its personal digital assistants bills, including:

- Requirements to maintain documentation that bills were reviewed, including certifications from those responsible for reviewing the bills.

- A description of how the reviews should be conducted, including what items to focus on and organization-wide thresholds for when to conduct detailed reviews of an individual's charges.

Management Response: MCC will develop a procedure for the monthly review of PDA bills by April 1, 2012.

Recommendation No. 2: We recommend that the Millennium Challenge Corporation's Chief Information Officer document and implement procedures (a) describing the required documentation that supervisors must submit for program officers and above and full-time personal service contractors to receive personal digital assistants and (b) requiring supervisors to periodically recertify (in a predefined time frame) staffs' continued need for personal digital assistants.

Management Response: MCC will develop guidelines consistent with the PDA policy outlining the requirements for staff to receive PDAs and a procedure requiring a documented business case for all staff that require PDAs. The procedure will require a semi-annual recertification process documenting the continued need for personal digital assistants. MCC will complete the guidelines and procedures associated with this recommendation by April 1, 2012.

Recommendation No. 3: We recommend that the Millennium Challenge Corporation's Chief Information Officer review and revise the Millennium Challenge Corporation's Policy on Personal Digital Assistants to reflect the Corporations current management position regarding the issuance of personal digital assistants to staff who are program officers and above and full-time personal service contractors.

Management Response: MCC will review and revise the MCC's Policy on Personal Digital Assistants to reflect the agency's current management position regarding the issuance of PDAs to staff who are program officers and above and full-time personal service contractors by December 30, 2011.

Recommendation No. 4: We recommend that the Millennium Challenge Corporation's Chief Information Officer prepare and implement documented procedures to (a) define what information is required to justify the need for a personal digital assistant for staff below the program officer level, contractors, and intermittent personal service contractors and (b) require supervisors to periodically recertify (in a predefined time frame) staffs' continued need for personal digital assistants.

Management Response: MCC will develop guidelines consistent with the PDA policy outlining the requirements for staff to receive and to continually possess PDAs by April 1, 2012.

Attachments:

IG/MCC, Lisa Banks
IG/MCC, Aleta Johnson
MCC/AF/FMD, Arlene McDonald
MCC/AF/FO, Mark Sandy