Privacy Impact Assessment for MCC Public Website

Submitted by:
Dennis Lauer, Chief Privacy Officer
Millennium Challenge Corporation (MCC)
875 15th Street N.W. Washington, DC 20005

December 1, 2010

MILLENNIUM
CHALLENGE CORPORATION
UNITED STATES OF AMERICA

Contents

Introduction

As part of its core requirement to engage with multiple external audiences, the Millennium Challenge Corporation (MCC) provides a means for its departments to engage with the public via the World Wide Web.

Therefore, MCC has developed a public facing website, described as "the System" in this document, to provide a means to effectively and efficiently disseminate information to the public, plan and execute public events, accept questions and requests for information, and accept feedback on a variety of topics, such as white papers, selection criteria methodology, and MCC's participation in the Administration's OpenGov initiative.

MCC's Department of Congressional and Public Affairs (CPA) has developed web forms as a part of the System in order to better capture event attendance requests and feedback from its users.

A Privacy Impact Assessment (PIA) is required, as the System collects Personally Identifiable Information (PII) from users who submit information via several web forms. Providing information using these web forms is completely voluntary, but the forms are the mechanism for the public to interact with MCC, to initiate whistleblower reporting, and to request to attend events at federal agencies, including MCC. In some cases, the user is not required to submit Pll in order to complete the form, such as in the comment and whistleblower forms.

Data in the System

What information is collected, used, disseminated, or maintained in the system?

Information collected in the System, is sensitive but unclassified, and non-exempt identifying information: First Name, Last Name, Street Address, City, State, Zip Code, Country, Telephone Number, Fax Number, Organization, Title, Email Address, Date of Birth, Driver's License Number, and Diplomatic Identification Number.

Information collected, used, and maintained by the System is for the following categories:

- ★ Individuals who are requesting to attend an MCC or Government event or function.
- ★ Individuals who provide comments or feedback to MCC.
- ★ Individuals who provide their information when completing the Whistleblower form.

None of this information is disseminated, except for that which is selectively shared with federal agency staff for event attendance at MCC or other Government agencies.

What are the sources of the information and how is the information collected for the project?

The System collects information via web form, directly from individuals who are requesting to attend an MCC or Government event, who submit a Request, Comments or Feedback to MCC, and/or by those who voluntarily provide their information when completing the Whistleblower form.

Why is the information being collected, used, disseminated, or maintained?

The System collects information from individuals desiring to attend an event at MCC or other Government agency hosting an event in which MCC is participating or has an interest. The information is necessary in order to process the individual for access to the event. In cases where the event is hosted at another Government agency, MCC shares the provided information with that agency for the sole purpose of facilitating access authorization.

The System also collects data from those individuals wishing to provide their contact information with regard to their Request, Comments or Feedback supplied to MCC and/or from when completing a Whistleblower form as part of the System if the individual desires to have further correspondence with or from MCC.

How is the information collected?

The System collects information via web forms that are completed and submitted by System users (web site visitors).

How will the information be checked for accuracy and timeliness?

System administrators have put in place reasonable checks to ensure completeness of the information provided by users. However, the System has no mechanism to determine the validity of the data. Users who discover errors in their submittal(s) may contact the website administrator to correct their information. As the provided information is voluntary, the user is responsible for ensuring that information is timely as it relates to event schedules, their desire to provide feedback to MCC, and so forth.

What law or regulation permits the collection of this information?

MCC operates under the Millennium Challenge Act of 2000--Public Law 108-199, Div. D, Title IV.

Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?

The privacy risks identified are that users who submit personally identifiable information (PII) may over-submit PII into the System and that this information could be accessed or utilized inappropriately.

These risks are mitigated by MCC's use of encryption of the information transmitted, role-based access controls that allow only appropriately trained MCC staff to access the information collected by the System, and by field and character limitations on the web forms that are submitted.

Use and Access to Data in the System

Describe how information in the system will or may be used.

The System utilizes information in the following manners:

1. Information that is submitted by users via on-line form for event attendance, Name, Organization, Title, Email Address, Date of Birth, Driver's License Number, and/or Diplomatic Identification Number, is submitted by the System administrator, to the extent that such disclosure is required to enable the hosting agency to make decisions concerning an individual's valid identification and background with regard to their attendance to an event or function.

2. In receipt of Requests/Comments/Feedback from the MCC community, Name and Email Address is used to respond back to a user's Request/Comment/Feedback.

3. In receipt of information submitted voluntarily by users via the on-line Whistleblower form; First Name, Last Name, Email Address, Street Address, City, State, Zip Code, County, Telephone Number, and Fax Number, may be used ifthe user so desires to engage with MCC directly to provide further information.

Which internal entities will have access to the information?

MCC Congressional and Public Affairs staff who are responsible for creating, securing, and gathering web form content are the only staff that will have access to the information.

Which external entities will have access to the information?

Externals entities have no direct access to the information. However, if the information collected is for an event hosted at another Government agency, MCC Congressional and Public Affairs staff will securely transmit it to the corresponding event or function hosting agency for vetting purposes only.

Notice and Access for Individuals

How will individuals be informed about what information is collected, and how this information is used and disclosed?

The System has a link to the MCC Privacy Policy at the bottom of each web page associated with the System that informs users submitting information via a web form about the collection, use, and disclosure of that information.

Do individuals have the opportunity and/or right to decline to provide information?

Yes. The information provided by individuals to the System is voluntary. The information is collected only as a result of being supplied by the user upon their completion and submittal of the web form(s) they opt to complete. For event attendance, the completion of fields on the associated web form may be required in order for an individual to be granted permission to attend an event by the associated Government entity.

Do individuals have the right to consent to particular uses of the information? If so, how would an individual exercise this right?

Yes. Individuals have the choice of whether or not they chose to fill out the fields on the System web form(s), and also have the choice of whether or not to consent and submit the information to MCC for use. MCC does not collect the information until it is submitted to MCC via a user's web form completion and verification of consent prior to submittal.

What are the procedures that allow individuals to gain access to their own information?

Individuals seeking access to non-public records must submit requests in writing to the MCC Chief Privacy Officer under the agency's Privacy Act access procedures.

Discuss the privacy risks associated with the process of providing individuals access to their own records and how those risks are mitigated.

The privacy risk of providing individuals access to records is that an individual could possibly gain access to the wrong record.

This risk is mitigated by the requirement for the individual to formally request access to their records, via the agency Chief Privacy Officer and Privacy Act procedure, wherein the individual would need to provide his/her full name, date of birth, and other proof of identity as required for Privacy Information Requests, detailed in the MCC Privacy Program policy.

Web Site Privacy Issues

Describe any tracking technology used by the website and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, Web beacon).

The System does not employ any tracking technologies such as temporary or persistent cookies.

If personal information is collected through the website, page, or online form accessible through the Internet, is appropriate encryption used? If not, explain.

Yes. Personally identifiable information (PII) is collected via web forms by the System. As PII is collected on the web forms, the information is transmitted via use of Transport Layer Security (TLS) using FIPS compliant cipher suites.

Explain how the public will be notified of the Privacy Policy

The System provides a prominent link the MCC Privacy Policy on all its web pages.

Considering any website or Internet issues, please describe any privacy risks identified and how they have been mitigated.

There is a privacy risk inherent in the transfer of Pll into and out of the System. This risk is mitigated by the agency's use of Transport Layer Security (TLS).

If the website will collect personal information from children under 13, or be directed at such children, explain how it will comply with the Children's Online Privacy Protection Act (COPPA).

The MCC website is not intended to collect any information from children under 13 years of age.

Security of Information in the System

Are all IT security requirements and procedures required by federal law being followed to ensure that information is appropriately secured?

MCC follows all Federal information Security Management Act (FISMA) requirements to ensure that information on the MCC website is appropriately secured. The information contained in the website is categorized as Moderate, (Sensitive but Unclassified), for confidentiality, integrity and availability, using the Federal Information Processing Standard (FIPS) 199.

Has a Certification & Accreditation been completed for the system or systems supporting the program?

A Certification and Accreditation (C&A) is currently in process for the System.

Has a risk assessment been conducted on the system?

A risk assessment is scheduled to be completed as part of the Certification and Accreditation process for the System that is currently ongoing.

Does the project employ technology that may raise privacy concerns? If so, please discuss its implementation.

The collection of PII *via* System web forms may raise a privacy concern. To alleviate this concern, PII is transmitted to the System from users via use of Transport Layer Security (TLS), a standard secure cryptographic information transfer method that is required for use by the Federal Government.

What procedures are in place to determine which users may access the system and are they documented?

MCC staff members responsible for maintaining the System have specified identification and password protected access to the System; access to the System is role-based and on a need-to-know and least privileged basis.

Describe what privacy training is provided to users either generally or specifically relevant to the program.

MCC staff complete Information Security and Privacy training when joining the agency. MCC staff also complete role-specific training, for those with access to PII. MCC staff adhere to yearly training certification requirements by completing Information Security and Privacy "tip-of-the-day" exercises which provide information, question, and answer responses to staff on a daily basis.

What auditing measures and technical safeguards are in place to prevent the misuse of data?

The System is audited in accordance with MCC Information System Security Policy. The Chief Information Security Officer (CISO) reviews and updates the policy annually to ensure it remains compliant with federal law, external mandates, and MCC business decisions.

Access to the System is role based and on a need-to-know and least privileged basis. MCC follows all Federal Information Security Management Act (FISMA) requirements, and PII is transferred only with the use of TLS, as stated in Office of Management and Budget (OMB) guidelines and in National Institute of Standards and Technology (NIST) 800-52.

Any questions regarding the security of the System should be directed to the MCC Chief Information Security Officer.

Data Retention

For what period of time will data collected in this system be maintained?

Pll in the form of Driver's License Number and Diplomatic Identification number, collected via web forms from individuals for event attendance is deleted 7 days after the information is supplied to the corresponding U.S. agency hosting an event. Additional Pll submitted by attendees (First Name, Last

Name, Street Address, City, State, Zip Code, Country, Telephone Number, Fax Number, Organization, Title, Email Address, Date of Birth) is deleted 60 days after the event occurs.

Data collected via System web form from individuals with regard to Requests/Comments/Feedback and/or Whistleblower forms is retained per MCC record retention policies.

What are the plans for destruction of disposal of the information?

The System is kept as a public MCC record per MCC record retention policies. PII in the form of Driver's License Number and Diplomatic Identification number collected from individuals for event attendance is deleted 7 days after the corresponding U.S. agency event occurs, and the remaining attendance information is disposed of 60 days after the event occurs; PII collected from individuals with regard to Requests/Comments/Feedback and/or Whistleblower forms are retained per MCC record retention policies.

Describe any privacy risks identified in the data retention and disposal of the information, and describe how these risks have been mitigated.

The privacy risk identified is that there could be an over-retention of data, or data retained in excess of its useful life. This risk is mitigated by the System administrator deleting event attendee records 60 days after the event occurs, and retaining all other data only as described in MCC record retention policies.

Privacy Act

Will the data in the system be retrieved by a personal identifier?

No, data in the System is not retrieved by a personal identifier.

Is the system covered by an existing Privacy Act System of Records Notice (SORN)?

MCC has created a SORN specific to this System and filed it with the Office of Management and Budget (OMB)- the Federal Register.

Privacy Policy

The collection, use, and disclosure of the information in this System have been reviewed to ensure consistency with the MCC Privacy Policy.

Approval

Responsible Officials

/s/ 12/1/2010
Dennis Lauer — Date
Chief Information Security Officer (Acting)
Millennium Challenge Corporation

/s/ 12/1/2010
Dennis Lauer — Date
Chief Information Officer/Chief Privacy Officer
Millennium Challenge Corporation