Privacy Threshold Analysis and Privacy Impact Assessment

Millennium Challenge Corporation – Public Website (MPW)

Version 1.4

May 2, 2017

Company Sensitive and Proprietary
For Authorized Use Only

Executive Summary

This document has been released originally in template format and is meant to be modified upon first use. Millennium Challenge Corporation – Public Website (MPW) is a Cloud Service Provider (CSP) offering that has undergone either a Privacy Threshold Analysis (PTA) or Privacy Impact Assessment (PIA). This document includes the PTA/PIA for Millennium Challenge Corporation – Public Website (MPW).

Document Revision History

Date	Description	Version	Author
03/2/2015	Final Version	1.0	ITG
03/13/2015	Updated Millennium Challenge Corporation – Amazon Web Services (MCC-AWS) to Millennium Challenge Corporation – Public Website (MPW)	1.1	ITG
02/12/2016	Updated mailing address in Table 2-1.	1.2	ITG
01/09/2017	Reviewed PTA/PIA per annual requirement. No changes were made.	1.3	ITG
5/2/2017	Updated CPO POC	1.4	ITG

Table of Contents

List of Tables

1. PRIVACY OVERVIEW AND POC

The following individual is identified as the Millennium Challenge Corporation Privacy Officer and point of contact.

Table 2-1. Millennium Challenge Corporation Privacy POC

Name	Vince Groh
Title	Chief Privacy Officer
CSP / Organization	Millennium Challenge Corporation
Address	1099 14th Street, NW Suite 700, Washington D.C. 20005
Phone Number	(202) 521-7265
Email Address	grohvt@mcc.gov

1.1. PRIVACY LAWS, REGULATIONS, AND GUIDANCE

A summary of laws, regulations related to privacy include:

- 5 U.S.C. § 552a, Freedom of Information Act of 1996, As Amended By Public Law No. 104-231, 110 Stat. 3048
- 5 U.S.C. § 552a, Privacy Act of 1974, As Amended
- Public Law 100-503, Computer Matching and Privacy Act of 1988
- E-Government Act of 2002 § 208
- Federal Trade Commission Act § 5
- 44 U.S.C. Federal Records Act, Chapters 21, 29, 31, 33
- Title 35, Code of Federal Regulations, Chapter XII, Subchapter B
- OMB Circular A-130, Management of Federal Information Resources, 1996
- OMB Memo M-10-23, Guidance for Agency Use of Third-Party Websites
- OMB Memo M-99-18, Privacy Policies on Federal Web Sites
- OMB Memo M-03-22, OMB Guidance for Implementing the Privacy Provisions
- OMB Memo M-07-16, Safeguarding Against and Responding to the Breach of PII
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- State Privacy Laws

Guidance on privacy issues can be found in the following publication:

- *NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing* http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

- FTC Fair Information Practice Principles
  http://www.ftc.gov/reports/privacy3/fairinfo.shtm

- Guidance on Managing Records in Cloud Computing Environments (NARA Bulletin)
  http://www.archives.gov/records-mgmt/bulletins/2010/2010-05.html

- Privacy and Security Law Issues in Off-shore Outsourcing Transactions
  http://www.outsourcing.com/legal_corner/pdf/Outsourcing_Privacy.pdf

1.2. PERSONALLY IDENTIFIABLE INFORMATION (PII)

Personally Identifiable Information (PII) as defined in OMB Memo M-07-16 refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Information that could be tied to more than one person (date of birth) is not considered PII unless it is made available with other types of information that together could render both values as PII (date of birth and street address). A non-exhaustive list of examples of PII include:

- Social Security numbers
- Passport numbers
- Driver's license numbers
- Biometric information
- DNA information
- Bank account numbers

PII does not refer to business information or government information that cannot be traced back to an individual person.

2. PRIVACY THRESHOLD ANALYSIS

Incentive Technology Group performs a Privacy Threshold Analysis annually to determine if PII is collected by any of the Millennium Challenge Corporation – Public Website (MPW) components. If PII is discovered, a Privacy Impact Assessment is performed. The Privacy Impact Assessment template used by Incentive Technology Group can be found in Section 3. This section constitutes the Privacy Threshold Analysis and findings.

2.1. QUALIFYING QUESTIONS

1) Does the Millennium Challenge Corporation – Public Website (MPW) collect, maintain, or share PII in any identifiable form?

☒ No
☐ Yes

2) Does the Millennium Challenge Corporation – Public Website (MPW) collect, maintain, or share PII information from or about the public?

☒ No
☐ Yes

3) Has a Privacy Impact Assessment ever been performed for the Millennium Challenge Corporation – Public Website (MPW)?

☒ No
☐ Yes

4) Is there a Privacy Act System of Records Notice (SORN) for this system?

☒ No
☐ Yes, the SORN identifier and name is: □□□□□

If answers to questions 1-4 are all "No" then a Privacy Impact Assessment may be omitted. If any of the answers to question 1-4 are "Yes" then complete a Privacy Impact Assessment.

2.2. DESIGNATION

☐ A Privacy Sensitive System

☒ Not a Privacy Sensitive System (in its current version)

3. PRIVACY IMPACT ASSESSMENT

A Privacy Impact Assessment has been conducted for the Millennium Challenge Corporation – Public Website (MPW) on January 9, 2017.

3.1. PII MAPPING OF COMPONENTS

Millennium Challenge Corporation – Public Website (MPW) consists of zero (0) key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Millennium Challenge Corporation – Public Website (MPW) and the functions that collect it are recorded in Table 4-1.

Table 4-1. PII Mapped to Components

Components	Does this function collect or store PII? (Yes/No)	Type of PII	Reason for Collection of PII	Safeguards
None – Zero (0)				

3.2. PII IN USE

1) What PII (name, social security number, date of birth, address, etc.) is contained in the CSP service offering? Explain. N/A – MPW does not collect PII

2) Can individuals "opt-out" by declining to provide PII or by consenting only to a particular use (e.g., allowing basic use of their personal information, but not sharing with other government agencies)? Explain. N/A – MPW does not collect PII

☐ Yes. Explain the issues and circumstances of being able to opt-out (either for specific data elements or specific uses of the data):

☒ No. Explain: N/A

3.3. SOURCES OF PII AND PURPOSE

3) Does the CSP have knowledge of federal agencies that provide PII to the system? Explain. N/A – MPW does not collect PII

4) Has any agency that is providing PII to the system provided a stated purpose for populating the system with PII? Explain. N/A – MPW does not collect PII

5) Does the CSP populate the system with PII? If yes, what is the purpose? Explain. N/A – MPW does not collect PII

6) What other third party sources will be providing PII to the system? Explain the PII that will be provided and the purpose for it. N/A – MPW does not collect PII

3.4. ACCESS TO PII AND SHARING

7) What federal agencies have access to the PII, even if they are not the original provider? Who establishes the criteria for what PII can be shared? Explain. N/A – MPW does not collect PII

8) What CSP personnel will have access to the system and the PII (e.g., users, managers, system administrators, developers, contractors, other)? Explain the need for CSP personnel to have access to the PII. N/A – MPW does not collect PII

9) How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Explain. N/A – MPW does not collect PII

10) Do other systems share, transmit, or have access to the PII in the system? If yes, explain the purpose for system to system transmission, access, or sharing. N/A – MPW does not collect PII

3.5. PII SAFEGUARDS AND LIABILITIES

11) What controls are in place to prevent the misuse (e.g., browsing) of data by those having access? Explain. N/A – MPW does not collect PII

12) Who will be responsible for protecting the privacy rights of the individuals whose PII is collected, maintained, or shared on the system? Have policies and/or procedures been established for this responsibility and accountability? Explain. N/A – MPW does not collect PII

13) Does the CSP annual security training include privacy training? Does the CSP require contractors to take the training? Explain. N/A – MPW does not collect PII

14) Who is responsible for assuring safeguards for the PII? Explain. N/A – MPW does not collect PII

15) What is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers be affected? Explain. N/A – MPW does not collect PII

16) What is the magnitude of harm to the individuals if privacy related data is disclosed, intentionally or unintentionally? Explain. N/A – MPW does not collect PII

17) What involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system? Explain. N/A – MPW does not collect PII

18) Is the PII owner advised about what federal agencies or other organizations share or have access to the data? Explain. N/A – MPW does not collect PII

3.6. CONTRACTS, AGREEMENTS, AND OWNERSHIP

19) NIST SP 800-144 states, “Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.” Is this principle described in contracts with customers? Why or why not? Explain. N/A – MPW does not collect PII

20) Do contracts with customers establish who has ownership rights over data including PII? Explain. N/A – MPW does not collect PII

21) Do contracts with customers require that customers notify the CSP if the customer intends to populate the service platform with PII? N/A – MPW does not collect PII

22) Do CSP contracts with customers establish record retention responsibilities for both the customer and the CSP? Explain. N/A – MPW does not collect PII

23) Is the degree to which the CSP will accept liability for expose of PII clearly defined in agreements with customers? N/A – MPW does not collect PII

3.7. ATTRIBUTES AND ACCURACY OF THE PII

24) Is the PII collected verified for accuracy? Why or why not? Explain. N/A – MPW does not collect PII

25) Is the PII current? How is this determined? Explain. N/A – MPW does not collect PII

3.8. MAINTENANCE AND ADMINISTRATIVE CONTROLS

26) If the system is operated in more than one site, how is consistent use of the system and PII maintained in all sites? Are the same controls be used? Explain. N/A – MPW does not collect PII

27) What are the retention periods of PII for this system? Under what guidelines are the retention periods determined? Who establishes the retention guidelines? Explain. N/A – MPW does not collect PII

28) What are the procedures for disposition of the PII at the end of the retention period? How long will any reports that contain PII be maintained? How is the information disposed (e.g., shredding, degaussing, overwriting, etc.)? Who establishes the decommissioning procedures? Explain. N/A – MPW does not collect PII

29) Is the system using technologies that contain PII in ways that have not previously deployed? (e.g., smart cards, caller-ID, biometrics, PIV cards, etc.)? Explain. N/A –

MPW does not collect PII

30) How does the use of this technology affect privacy? Does the use of this technology introduce compromise that did not exist prior to the deployment of this technology? Explain. N/A – MPW does not collect PII

31) Is access to the PII being monitored, tracked, or recorded? Explain. N/A – MPW does not collect PII

32) If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision? Explain. N/A – MPW does not collect PII

3.9. BUSINESS PROCESSES AND TECHNOLOGY

33) Does the conduct of this PIA result in circumstances that requires changes to business processes? Explain. N/A – MPW does not collect PII

34) Does the completion of this PIA potentially result in technology changes? Explain. N/A – MPW does not collect PII

3.10. PRIVACY POLICY

35) Is there a CSP privacy policy and is it provided to all individuals whose PII you collect, maintain or store? Explain. N/A – MPW does not collect PII

36) Is the privacy policy publicly viewable? N/A – MPW does not collect PII

3.11. CHIEF PRIVACY OFFICER SIGNATURE

This Privacy Impact Assessment has been conducted by ITG and has been reviewed by the Chief Privacy Officer for accuracy.

Digitally signed by Vincent T Groh
Date: 2017.05.10 10:10:02 -04'00'

Chief Privacy Officer Signature

Date

3.12. ACRONYMS

Acronym	Definition
CSP	Cloud Service Provider
HIPAA	Health Insurance Portability and Accountability Act
IT	Information Technology
NIST	National Institute for Standards and Technology
OMB	Office of Management and Budget
POC	Point of Contact
PII	Personally Identifiable Information
PTA	Privacy Threshold Analysis
SORN	System of Records Notice