MILLENNIUM
CHALLENGE CORPORATION
UNITED STATES OF AMERICA

Privacy Impact Assessment
Millennium Challenge Corporation (MCC) Network (MCCNet)

December 31, 2009
Version 1.1

Submitted by:

Stanley Associates / Iron Vine Security

Millennium Challenge Corporation

875 15th Street N.W.

WASHINGTON, DC 2000

ACTION:	APPROVER:	SIGNATURE:	DATE:
APPROVAL:	Dean Ergenbright, MCC Chief Privacy Officer		December 31, 2009

TABLE OF CONTENTS

1 Definitions

1.1   **MCCNet System.** The MCCNET system includes the hardware and software needed to provide the MCCNet (i.e., the routers, switches, policy enforcement platform, event database, correlation engine and web interfaces).

1.2   **Flow.** Flow is a computer network traffic summarization format widely used by network engineers and security analysts. It summarizes communication between two hosts communicating over the Internet.

1.3   **Collect/Collection.** As used herein, to collect or collection means to gather, or accumulate, or to recover or take control over.

1.4   **System of Record.** A group of records that are retrieved by some kind of personal identifier, such as a name or number.

1.5   **Electronic Storage.** As used herein, to store has the meaning used in the 18 U.S.C § 2510, *i.e.,* "**(A)** any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and **(B)** any storage of such communication by an electronic communication service for purposes of backup protection of such communication".

2 PIA Contacts and Overview

2.1 Contact Information

System Title: **Millennium Challenge Corporation Network General Support System**
Acronym: **MCCNet GSS**

Office of Responsibility:
   MCC/Administration and Finance
   Office of the CIO
   875 15th Street NW
   Washington, DC 20005

   The System is maintained by:
   Computer Science Corporation (CSC)
   Newark Data Center
   645 Paper Mill Road
   Newark, Delaware 19711

Enter the information for the System Owner

   Name: Dennis Lauer
   Title: MCC Chief Information Officer
   Street: 875 15th Street NW
   City: Washington   State: DC   Zip Code: 20005
   Telephone: 202-521-7527
   Email: lauerd@MCC.gov

Signature: **Date:**

Enter the information for other designated contacts for the system

   Name: Michael Casella
   Title: Acting Vice President, Administration and Finance
   Street   Address: 875 15th Street NW
   City: Washington   State: DC   Zip Code: 20005
   Telephone: 202-521-3723
   Email: casellam@MCC.gov

Enter the information for the Chief Privacy Officer

Name: Dean Ergenbright
Title: Deputy CIO and Chief Privacy Officer
Street: 875 15th Street NW
City: Washington   State: DC   Zip Code: 20005
Telephone: 202-521-7230
Email: ergenbrightde@MCC.gov

Enter the information for the Information System Security Officer

Name: Trey Carr
Title: Chief Information Security Officer
Street: 875 15th Street NW
City: Washington   State: DC   Zip Code: 20005
Telephone: 202-521-2688
Email: carrwh@MCC.gov

2.2 Overview

The Millennium Challenge Corporation Network (MCCNet) system is currently operational. MCCNet is a General Support System, which is comprised of four main sites with high speed communications links. As currently configured, the network supports approximately 410 users.

The Office of Management and Budget (OMB) requires agencies to conduct Privacy Impact Assessments for electronic information systems and collections and, in general, make them publicly available. OMB provides guidance to agencies on implementing the privacy provisions of the E-Government Act of 2002 in OMB M-03-22. This guidance allows agencies the flexibility of determining the depth and content of a PIA. In addition, M-03-22 allows the development of standardized forms and templates for completing PIA's. This PIA format was developed to meet the requirements of the E-Gov Act of 2002 as outlined in M-03-22.

Memorandum 03-22 identified eight topics that must be covered within the content of a PIA. They are as follows:

1. Information to be collected
2. Reason for the collection of the information
3. Intended use of the information collected
4. The sharing of the information
5. Declining or consenting to provide the information
6. Securing the information
7. Creating a system of records under the Privacy Act, 5 U.S.C. 552a
8. Any choices that the agency made regarding an IT system or collection of information as a result of performing the PIA

The MCC Privacy Office developed this PIA template to respond to the eight topics. The MCC Privacy Office reserves the right to request clarification, supporting documentation or expanded answers to these questions before determining whether approval is granted. The information provided in the PIA is final product of an analysis of information by the system owner, based on information received and discussed between various system stakeholders, such as developers, users, managers, system ISSO or IT project managers.

3 Collection of Information

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

The information collected, used, disseminated or maintained within the MCCNet system is as follows:

- Employee files maintained within Human Resources
- Payroll information
- Investigations and Clearance Tracking System database - full identifying info to include name, DoB, PoB, SSN and security clearance info
- Security forms completed by individuals to include completed SF 86s and SF 85Ps, and signed releases of information
- Copies of Reports of Investigations
- Photos of all employees and contractors (Privacy Act controlled)

3.2 Why is the information being collected, used, disseminated, or maintained by the MCCNet system?

The MCCNet system supports the Agency's automated business processes for budgeting, planning, procurement, contracts monitoring and awards, tracking results and performance, and administrative functions. Additionally, MCCNet collects, uses, disseminates, or maintains this information to protect MCC personnel and data, and to meet the Agency objectives.

4 Uses of the Information

4.1 How will the information be used?

The personnel information collected is used to screen direct hires and contractors for the purpose of hiring personnel complying with the appropriate regulations. Additionally, privacy information may be collected for payroll purposes; and investigation purposes for either security clearances or security incidents.

4.2 With whom will this information be shared?

The personnel and payroll information will be shared with the Department of Interior National Business Center.

4.3 What opportunities do individuals have to decline to provide the information and how can individuals grant consent?

Notice is given to the individual prior to the collection of the information.

5   Securing the Information

5.1   How is the information secured?

The information is secured using many computer security technologies, including: Firewalls, Network Vulnerability Scans, FDCC Controls, Intrusion Detection Sensors, and Virtual Private Networks.

5.2   What Security Controls are in Place to Protect the Information?

The MCCNet system has various security controls in place to protect privacy information. MCCNet uses a combination of Access Controls and User Identification and Authentication controls to protect the MCC information.

6   System of Records Notice

6.1   Will a system of records be created or updated under the Privacy Act, 5 U.S.C. 552a?

A system of records notice has not been created for the MCCNet system.

7   Resulting Decisions

7.1   What choices did the agency make regarding MCCNet or the collection of information as a result of performing the PIA?

MCC is conducting an assessment of PII information that is in use at MCC. This assessment is being conducted as part of a larger enterprise content management project and will be used to document all locations where PII and Social Security Numbers are in use at MCC.