PRIVACY IMPACT ASSESSMENT

ORC

February 18 2015

Part I: PIA Qualification Questions

A. Qualification Questions

Question	Explanation / Instructions
1. Does your system collect any information in identifiable form (personal data) on the general public? (YES or NO. If YES, a PIA is required, starting in FY 2004.)	**No**
2. Does your system collect any information in identifiable form (personal data/information) on government employees? (YES or NO. If YES, a PIA is required, starting in FY 2005.)	**Yes**
3. Has a PIA been done before for the system? (YES or NO)	**Yes**

Part II: PIA Data

A. Data in the System

Question	Explanation/Instructions
1. Describe all information to be included in the system, including personal data.	a. The system provides credentials to Federal employees and contractors as authorized by Federal Government sponsors (e.g. FEC, FTC). b. For each individual, the system may contain the following data elements: Name, Date of Birth, E-mail address (work), Driver's License Number, Biometrics, Military ID (if applicable), Passport Number, Social Security Number. Collection of each individual's information is performed by designated Government personnel at the Government facility (e.g. FEC, FTC).
1.a. What stage of the life cycle is the system currently in?	Operation/Maintenance
2.a. What are the sources of the information in the system?	The information is entered by designated Government personnel authorized to access the system.
2.b. What GSA files and databases are used?	None.
2.c. What Federal agencies are providing data for use in the system?	Federal Trade Commission Federal Election Commission
2.d. What State and local agencies are providing data for use in the system?	None.
2.e. What other third party sources will the data be collected from?	None.

Question	Explanation/Instructions
2.f. What information will be collected from the individual whose record is in the system?	For each individual, the system may contain the following data elements: Name, Date of Birth, E-mail address (work), Driver's License Number, Biometrics, Military ID, Passport Number, Social Security Number.
3.a. How will the data collected from sources other than Federal agency records or the individual be verified for accuracy?	Not applicable.
3.b. How will data be checked for completeness?	The card issuance application is designed to require that all data fields be completed prior to allowing the process to proceed to the next step. Failure to complete all required fields results in an error response (e.g. "the following fields must be completed").
3.c. Is the data current? How do you know?	The designated Government individual responsible for entering the data of the applicant is trained to verify that all identity credentials provided are (a) from the approved list of identity documents, (b) match the identity of the applicant, and (c) are unexpired.
4. Are the data elements described in detail and documented? If yes, what is the name of the document?	Yes. ORC SSP customers possess a *Registration Practices Statement (RPS)* developed in collaboration with ORC.

B. Access to the Data

Question	Explanation/Instructions
1. a. Who will have access to the data in the system?	Access to system data is restricted to authorized roles (Certification Authority Administrators; System Administrators; System Registrars; System Issuers, System Sponsors). There is no public access to the data in the system.
1.b. Is any of the data subject to exclusion from disclosure under the Freedom of Information Act (FOIA)? If yes, explain the policy and rationale supporting this decision.	Information requested from individuals during the certificate issuance process other than that information, which is specifically included in the certificate, is withheld from release. This information may include personal information and is subject to the Privacy Act. All information in the ORC SSP record (not repository) is handled as SBU, and access will be restricted to those with official needs. (FOIA Exemption 7(C))

Question	Explanation/Instructions
2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?	Information requested from individuals during the certificate issuance process other than that information, which is specifically included in the certificate, is withheld from release. This information may include personal information and is subject to the Privacy Act. All information in the ORC SSP record (not repository) is handled as SBU, and access will be restricted to those with official needs. (FOIA Exemption 7(C))
3. Will users have access to all data in the system or will the user's access be restricted? Explain.	Users do not have access to data in the system.
4. What controls are in place to prevent the misuse (e.g. browsing) of data by those having access?	Only those individuals in trusted roles (Certification Authority Administrators; System Administrators; Registrars; Issuers, Sponsors) have access to data in the system. Individuals holding these roles attest to the obligations of their respective role and adherence to all policies and procedures governing the protection of private data by means of an appointment letter, which they sign prior to gaining access to perform their role.
5.a. Do other systems share data or have access to data in this system? If yes, explain.	No other systems have access to the data in this system.
5.b. Who will be responsible for protecting the privacy rights of the clients and employees affected by the interface?	N/A
6.a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?	No.
6.b. How will the data be used by the agency?	N/A.
6.c. Who is responsible for assuring proper use of the data?	N/A
6.d. How will the system ensure that agencies only get the information they are entitled to?	N/A
7. What is the life expectancy of the data?	Per the Certification Practices Statement, retention of data is required for 10 years and 6 months.
8. How will the data be disposed of when it is no longer needed?	Prior to the end of the archive retention period, ORC will provide archived data to a Policy Authority approved archival facility, upon request. ORC could itself own that facility. If retention is no longer needed, either the Policy Authority will properly dispose of the archived data or ORC will dispose of the archived data following approved data destruction methods (e.g. NIST SP800-88 or DOD NISPOM).

C. Attributes of the Data

Question	Explanation/Instructions
1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?	Yes. PII data collected is relevant and necessary in order for the ORC SSP system to generate accurate and current PIV cards to be relied upon by Federal systems, both physically and logically.
2.a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?	Yes, the Card Holder Unique Identifier (CHUID).
2.b. Will the new data be placed in the individual's record (client or employee)?	Yes
2.c. Can the system make determinations about individuals that would not be possible without the new data?	No. The CHUID is derived solely from the existing information. Nothing new is generated other than the CHUID itself.
2.d. How will the new data be verified for relevance and accuracy?	Since this is privacy data about an individual that was not provided by the individual, the relevance and accuracy is very important. Provide details on processes used to verify this information.
3.a. If the data is being consolidated, what controls are in place to protect the data and prevent unauthorized access? Explain.	N/A
3.b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.	N/A
4. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.	The data can only be retrieved by authorized individuals (Sponsor, Registrar, Issuer) authenticating to an SSP workstation connected to the Card Management System (CMS) via secure (SSL) connection.
5. What are the potential effects on the privacy rights of individuals of: a. Consolidation and linkage of files and systems; b. Derivation of data; c. Accelerated information processing and decision making; and d. Use of new technologies. How are the effects to be mitigated?	a. The PII of individuals is not linked to any other systems. b. The only data that can be derived for the system by anyone other than those individuals in trusted roles is the publicly available information (public keys; CRLs) c. N/A d. N/A

D. Maintenance of Administrative Controls

Question	Explanation/Instructions
1.a. Explain how the system and its use will ensure equitable treatment of individuals.	Describe the processes in place to ensure fair and equitable treatment of individuals and their privacy data. If judgments are to be made based on the privacy data, indicate the rationale to be used to make the judgments and how the judgments will be kept fair and equitable.
1.b. If the system is operated in more than one site, how will consistent use of the system be maintained at all sites?	N/A. The ORC SSP CA and CMS only reside at the ORC facility in the Secure Network Operations Center.
1.c. Explain any possibility of disparate treatment of individuals or groups.	Describe any potential situation where data could be evaluated differently. List the data elements that may impact disparate treatment (i.e. race, gender, etc) N/A. For ORC SSP, all applicant data it evaluated and protected to the same level.
2.a. What are the retention periods of data in this system?	How long will data be kept (years, months, day, hours). Use GSA records disposition schedules to determine requirements. Per the Certification Practices Statement, data is retained for ten (10) years and six (6) months prior to allowable destruction following approved GSA methods.
2.b. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?	Provide detailed explanation of the data disposal process. Indicate methods for disposing of data from operational databases as well as archiving procedures. List documents supporting these procedures and the locations of these documents. ORC SSP data disposal is performed using the services of Securis©. Securis© is fully compliant with NIST SP800-88 and the DOD NISPOM and are the commercial contactor for the destruction of all IT hardware devices in accordance with industry best practices.[1]
2.c. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?	Period testing of backup data, performed annually at a minimum.
3.a. Is the system using technologies in ways that Federal agencies have not previously employed (e.g. Caller-ID)?	No

[1] Securis holds a contract with the Federal Government under General Services Administration (GSA). The schedule is 36 and contractor number is GS-03F-0068V. This contract is for on-site and off-site shredding services, degaussing services and computer recycling. Securis is also certified by the Defense Logistics Information Service to store and transport military critical technical data. Securis' certification number is 0051653 and expires May 15, 20 - See more at: http://www.securis.com/data-destruction/e-waste-recycling/certifications-and-compliance/#sthash.DLhJ4Bk5.dpuf

Question	Explanation/Instructions
3.b. How does the use of this technology affect individuals' privacy?	N/A
4.a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	No.
4.b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.	No.
4.c. What controls will be used to prevent unauthorized monitoring?	Not applicable.
5.a. Under which Privacy Act System of Records notice (SOR) does the system operate? Provide number and name.	Part IV Federal Trade Commission, Privacy Act of 1974, Systems of Records; Notice; (FTC-VII-3 (Computer Systems User Identification and Access Records—FTC).
5.b. If the system is being modified, will the SOR require amendment or revision? Explain.	Part IV Federal Election Commission, Privacy Act of 1974, Systems of Records; Notice; (FEC 16 HSPD–12: Identity Management, Personnel Security, Physical and Logical Access Files).

Signature Page

X

William Morgan
Information System Security Officer

X

Jonathan Wallick
Information System Security Manager

X

Chi Hickey
Program Manager

X

Kim Mott
GSA PIA Officer