Status: Final

Form Date: 30-SEP-13

Question 1: OPDIV
Question 1 Answer: OS

Question 2: PIA Unique Identifier (UID):
Question 2 Answer: P-2277902-798208

Question 2A: Name:
Question 2A Answer: Identity and Access Management System at HHS

Question 3: Which of the following objects does this PIA Cover?
Question 3 Answer: Major Application

Question 3A: Identify the Enterprise Life-Cycle Phase of the System:
Question 3A Answer: Operations and Maintenance

Question 3B: Is this a FISMA Reportable System?
Question 3B Answer: Yes

Question 4: Does the system include a publicly available Web interface?
Question 4 Answer: No

Question 5: Identify the operator
Question 5 Answer: Contractor

Question 7: Is this a new or existing system
Question 7 Answer: Existing

Question 8: Does the system have Security Authorization (SA)?
Question 8 Answer: Yes

Question 8A: Date of Security Authorization
Question 8A Answer: 09-MAY-12

Question 9 : Indicate the following reason(s) for updating this PIA.
Choose from the following options.
PIA Validation (PIA Refresh/Annual Review): Checked
Significant System Management Change: Not Checked
Anonymous to Non-Anonymous: Not Checked
Conversion: Not Checked
New Public Access: Not Checked
New Interagency Uses: Not Checked
Internal Flow or Collection: Not Checked
Alteration in Character of Data: Not Checked
Commercial Sources: Not Checked

Question 10: Describe in further detail any changes to the system that have occurred since the last PIA.
Question 10 Answer: The application has had several software releases. Additionally, OS patching occurs quarterly

Question 11: Describe the purpose of the system.
Question 11 Answer: Purpose of this system is to meet HSPD-12 requirements to provide physical and logical

Identity and Access Management within HHS.

The IAM@HHS is a department-wide solution to issue PIV credentials to HHS employees and contractors and perform identification and authentication of local and remote users to allow access to HHS applications. The system will provide access and identity management for all users of HHS IT systems.

Question 12: Describe the type of information the system will collect, maintain (store), or share. (Subsequent questions will identify if this information is PII and ask about the specific data elements.)
Question 12 Answer: The agency will collect the following PII information: full name, facial photograph, fingerprints, date of birth, home address, home phone number, background investigation form, the results of a background check, the approval signature of the person who registered the user in the system, card expiration date, the card serial number, and copies of the documents used to verify identity, such as driver's license or passport. Data is collected for all HHS employees (federal and contractors).

Mandatory submissions - The investigation is a federal government job requirement. Those who refuse to provide personal information will not meet the requirements of the job and will therefore not be considered further. Current employees who do not meet these requirements will be terminated.

Question 13: Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.
Question 13 Answer: IAM is a system that supports the HHS Homeland Security Presidential Directive HSPD-12 program. Its functions will allow HHS to produce the new ID badges that will be required for all HHS employees and contractors across all HHS Operating Divisions (OpDivs). The PII collected will be used to uniquely identify personnel on Personal Identity Verification (PIV) cards. This information includes biometrics (fingerprints) and digital certificates. This system was authorized by the HHS CIO and meets Presidential Directive HSPD-12 guidance.

IAM is actually a suite of three systems, described below. It provides enrollment services (creating records and accounts of individuals), a centralized Personal Identity Verification (PIV) Smart Card Management System (controlling the issuing of PIV cards to individuals), local card production facility support, card activation, finalization and issuance. The HHS HSPD-12 program also provides logical access to HHS Enterprise applications (through AMS) and physical access to those HHS facilities that are integrated with the SecureSAFE solution.

1. Smart Card Management System (SCMS) - The SCMS manages and protects secure data about individuals/applicants and links to third-party systems to evaluate individuals' security status, providing up-to-date information about individuals who should be granted or denied access to HHS facilities and/or information systems. The SCMS is the "identity store," a resource that establishes an identity record for each individual. The records contain each individual's official identity information, including required biographic and biometric data, sponsorship and employer data, and adjudication results of background investigations. The SCMS collects data elements from the PIV card applicant, including name, date of birth, Social Security Number, organizational and employee affiliations, fingerprints, digital color photographs, work e-mail addresses, and phone numbers, as well additional verification and demographic information (like the results of background investigations). The SCMS provides management of the various credential types, the cardholder data, and the card lifecycle. Main functionalities include:

- Requesting, distribution, and administration of cards;
- Card lifecycle and profile management;
- Data preparation for loading, installing, and personalization of cards;
- Visual personalization (photographs, etc.).

2. SecureSAFE - The HSPD-12 program follows a service-oriented architecture (SOA) approach in the transmission and exchange of applicant data (i.e., data about individuals who have been issued PIV cards) to and from various OPDIV Physical Access Systems (PACS). The SAFE application performs the synchronization and near real-time updates of identities from the SCMS, including updates of personal or credential information, handling expired or revoked PIV certificates, and the provisioning of new PIV holders. SecureSAFE enables security managers to create processes and policies to grant, manage, revoke, and

provision physical security identities and access privileges even in an environment of disparate PACS vendors and technologies.

3. Access Management Systems (AMS) - AMS provides various benefits that enhance the user's experience by reducing the number of usernames and passwords users need to memorize, supporting multiple authentication methods (e.g. password, PIV card), limiting exchange/proliferation of user credentials, and enabling a consistent program-wide authentication service. The core AMS architecture implements a strong Identity and Access Management framework that provides user management, self-service, and authentication and authorization services. In addition, AMS provides robust identity management capabilities such as the ability to integrate OPDIV Active Directories and the SCMS with the HSPD-12 System. AMS provides HHS several functions which include Simplified Sign-On (SS

Question 14: Does the system collect, maintain, use, or share PII?
Question 14 Answer: Yes

Question 15 : Indicate the type of PII that the system will collect or maintain.
Indicate the type of PII the system will collect or maintain.
Social Security Number: Checked True
Date of Birth: Checked True
Name: Checked True
Photographic Identifiers: Checked True
Driver's License Number: Checked True
Biometric Identifiers: Checked True
Mother's Maiden Name: Not Checked
Vehicle Identifiers: Not Checked
Mailing Address: Checked True
Phone Numbers: Checked True
Medical Records Number: Not Checked
Medical Notes: Not Checked
Financial Accounts Info: Not Checked
Certificates: Not Checked
Legal Documents: Not Checked
Education Records: Not Checked
Device Identifiers: Not Checked
Military Status: Not Checked
Employment Status: Checked True
Foreign Activities: Not Checked
Q15 Other 1: Place of birth, Unique identifier (card serial number)

Question 16 : Q6
Indicate the categories of individuals about whom PII is collected, maintained, or shared.
Employees: Checked True
Public Citizens: Not Checked
Business Partner/Contacts (Federal/state/local agencies: Not Checked
Vendor/Suppliers/Contractors: Checked True
Patients: Not Checked
Q16 Other: none

Question 17: How many individuals' PII is in the system?
Question 17 Answer: 100,000-999,999

Question 18: For what purpose is PII used?
Question 18 Answer: HHS will use the information when individuals access federal facilities, computers, applications, or data to prove the individual's identity and right of access. Information is shared with OPM for clearance of employees, with the certification authority which provides digital certificates, and with the

Federal Bridge Certification Authority (CA), an organization established to create a federal bridge using Commercial-Off-The-Shelf products to bind Agency PKIs together, ensure directory compatibility. Ultimately, PII will also be shared with other federal agencies to facilitate agency collaborations by allowing federal staff to enter other facilities, with permission. PII will also be shared with other systems that will interact with IAM to permit use of those services under SSO.

IAM will facilitate single sign-on (SSO) to many HHS systems. Initially, these systems will include HHSNet, Enterprise Human Resources and Personnel (EHRP), Enterprise Workflow Information Tracking System (EWITS), Payment Management System (PMS),One Stop Service (OSS), Integrated Time and Attendance System (ITAS), Business Intelligence Information System (BIBS), ACF SSI, NIH Sharepoint, GAL/ADAM, People Processing System, HHSIdentity/NED, Computer-Controlled Access (CCA), Parklawn Physical Access Control System (PACS), FDA PACS, SAMHSA PACS, NIH login / federated ID Service, HSPD-12Virtual Directory (six instances at NIH, CMS, CDC, IHS, ASA/ACF/AHRQ/AOA/SAMHSA, and HRSA) HHS Enterprise Architecture Repository (HEAR), GovNet-NG, Managing & Accounting Credit Card System (MACCS), and Enterprise Portal.

SSO will also be available to many systems owned or operated by other agencies or contractors on behalf of HHS to conduct HHS services. These include Learning Management System (LMS, at the Office of Personnel Management (OPM)), Verizon CA (Verizon as a contractor for the General Services Administration (GSA)), FTS (OPM), Card Production (Contractor Oberthur

Question 19: Describe secondary uses for which PII will be used (e.g. testing, training or research)
Question 19 Answer: N/A

Question 20: Describe the function of the SSN.
Question 20 Answer: The SSN is used for initial user authentication and matching resource access privileges to HR applications.

Question 20A: Describe the function of the SSN.
Question 20A Answer: There is no specific legal authority for use of the SSN, but the use of a widely-used, externally-verifiable unique identifier is critical to the effective implementation of HSPD-12. Currently, HHS is not aware of another identifier that meets our requirements.

Question 21: Describe secondary uses for which PII will be used (e.g. testing, training or research)
Question 21 Answer: HSPD-12 requires the implementation of systems and processes that "enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees)."

Question 22: Describe secondary uses for which PII will be used (e.g. testing, training or research)
Question 22 Answer: Yes

Question 22A-3B: SORN #3
Question 22A-3B Answer: GSA/GOVT-7

Question 23A: Identify the OMB information collection approval
number and expiration date
Question 23A Answer: N/A

Question 23 : Identify the sources of PII in the system.
Identify the sources of PII in the system.
Directly from an individual about whom the information pertains.
In Person: Checked True
Online: Checked True
Government Sources
Within the OPDIV: Checked True
Other Federal Entities: Not Checked

Question 24: Is the PII shared with other organizations?
Question 24 Answer: No

Question 25: Describe the process in place to notify individuals that their personal information will be collected.
If no prior notice is given, explain the reason.
Question 25 Answer: Individuals will be aware of what information is collected because they will be required to provide their information directly as part of the onboarding process. They will provide the information via a standard form (SF), SF 745.

Individuals will be aware of the purpose of submitting the information, which will be to request assignment of an access badge. Opportunities to further understand the use of their PII will occur during the completion of the eQIP profile, including the provision of background information.

Question 26: Is the submission of PII by individuals voluntary or mandatory?
Question 26 Answer: Mandatory

Question 27: Describe the method for individuals to opt-out of collection or use of theri PII.
If there is no option to object to the information collection, provide a reason.
Question 27 Answer: The investigation is a federal government job requirement. Those who refuse to provide personal information will not meet the requirements of the job and will therefore not be considered further. Current employees who do not meet these requirements will be terminated.

Individuals submit their PII during the eQIP background screening process. They are informed that by signing the completed eQIP form and submitting it, they are authorizing HHS to verify the information provided as a condition of being permitted security clearance to work at their assigned tasks.

Question 28: Describe the process to notify and maintain consent from the individuals whose PII is in the system.
Question 28 Answer: In cases involving individuals or small groups of users, notifications of major changes will be delivered via individual e-mails. In cases involving a large amount of users a mass email will be sent via distribution lists informing users of what has occurred, and their options, if there are any resulting procedural or privacy changes. Incidents will also be reported to the HHS Secure One Help Desk and resolved in a timely fashion.

Question 29: Describe the process in place to resolve an individual's concerns when they believe their PII has
been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. If no process exists, explain
why no.
Question 29 Answer: Individuals should contact their Chief Information Security Officers (CISOs) if they believe their PII has been inappropriately obtained, is incomplete or inaccurate, or is being misused. Individuals are informed of the proper procedures to follow in these circumstances during security and privacy training, which they are required to complete annually.

Question 30: Describe the process in place for periodic reviews of PII contained in the system to ensure the data's
integrity, availability, accuracy and relevancy. If no processes are in place, explain why not.
Question 30 Answer: HHS will periodically require individuals to update and verify the background information provided as a condition of re-issuing individual ID cards.

Question 31 : Identify who will have access to the PII in the system and the reason why they require access.
Identify who will have access to the PII in the system and the reason why they require access.

User Check Box: Checked True
User Reason: To enter PII for enrollment or card issuance.
Administrators Check Box: Checked True
Administrator Reason: To ensure the smooth operation of the system.
Developers Check Box: Checked True
Developers Reason: To debug system problems, routine maintenance.
Contractors Check Box: Checked True
Contractors Reason: If acting in the role of an administrator

Question 32: Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII
Question 32 Answer: The system makes extensive use of roles, rights, and privileges to enforce access to PII.

Question 33: Describe the methods in place to allow those with access to PII to only access the minimum amount of
information necessary to perform their job.
Question 33 Answer: Access to PII is on a need-know basis, and derived by job role and access privileges.

Question 34: Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities
for protecting the information being collected and maintained.
Question 34 Answer: Personnel must attend all applicable federal privacy training. In addition, contractors attend additional PII training beyond that what is required by the Federal government.

Question 35: Describe training system users receive (above and beyond general security and privacy awareness
training).
Question 35 Answer: Internal system training is available via role-based training presentations posted on the Intranet and on-the-job training. Both review PII concepts and security procedures to ensure personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Question 36: Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to
privacy provisions and practices.
Question 36 Answer: Yes

Question 37: Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite
specific records retention schedules.
Question 37 Answer: Records are retained in accordance with General Records Schedule (GRS) 18, Item 17. Unless retained for specific ongoing security investigations, records of access are maintained for five years for maximum security facilities and then destroyed. Records are maintained for two years for other facilities and then destroyed.

All other records relating to individuals are retained and disposed of in accordance with GRS 18, Item 22a.

In accordance with HSPD-12, PIV Cards are deactivated within 18 hours of cardholder separation, loss of card, or expiration. The information on PIV Cards is maintained in accordance with GRS 11, Item 4. PIV Cards are destroyed by cross-cut shredding no later than 90 days after deactivation.

Question 38: Describe, briefly but with specificity, how the PII will be secured in the system using administrative,
technical, and physical controls.
Question 38 Answer: The database and individual OPDIV feeder servers are located within secured buildings.

Different degrees of security have been implemented at all locations, with some including biometrics and closed circuit TV.

Technical controls which minimize the possibility of unauthorized access, use, or dissemination of the data in the system are also in place. These include: user identification, firewalls, VPN, encryption, Intrusion Detection System and PIV Cards.

Guards, ID Badges and Key cards further ensure PII will be secure.

Question 39: Identify the publicly-available URL:
Question 39 Answer: http://iam.hhs.gov