Status: Final

Form Date: 21-JAN-15

Question 1: OPDIV
Question 1 Answer: OS

Question 2: PIA Unique Identifier (UID):
Question 2 Answer: P-1517605-175615

Question 2A: Name:
Question 2A Answer: HHS Email as a Service

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: Requirements Analysis

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: New

Question 8: Does the system have Security Authorization (SA)?
Question 8 Answer: No

Question 8B: Planned Date of Security Authorization
Question 8B Answer: 10-APR-15

Question 8B-1: Planned date of Security Authorization - Not Applicable
Question 8B-1 Answer: Not Checked

Question 8C: Breifly explain why security authorization is not required
Question 8C Answer: ATO is required, but the system is in very early stages of the Enterprise Performance Life Cycle, and a date for ATO is not yet projected.

Question 11: Describe the purpose of the system.
Question 11 Answer: The Department of Health and Human Services (HHS) is establishing a cloud computing Software as a Service (SaaS) solution for email, collaboration, and communication tools (hereafter, referred to as Email as a Service or EaaS) which leverages the Microsoft Government-only cloud. The cloud services align with the descriptions provided by the National Institute of Standards and Technology (NIST) in Special Publication 800-145.

The primary purpose of HHS EaaS is to leverage a Government Community Cloud (GCC) solution to obtain improvements in continuity operations, collaboration, efficiency, agility, innovation, and cost savings, for email and office productivity services previously provided by its enterprise email applications and existing collaboration solutions.

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 e-mail system does not collect or request specific PII data; however, there is a possibility of the exchange of PII data between individuals or groups of individuals through the transmission of e-mail messages. These messages could be stored for retrieval in a user's mailbox or personal archives indefinitely as well as retained in storage arrays for 14 days which is the HHS e-mail retention policy.

E-mails are transmitted between HHS employees for normal day to day business operations but PII data is never explicitly collected or used by the system (i.e., there are no forms or fields for PII collection, and PII collection is not the explicit purpose of the system).

The EaaS system itself does not include an Active Directory server within it's ATO boundary, but interconnects to the existing Active Directory infrastructure in order to manage and authenticate users' access to their mailboxes. As a result, Active Directory field data requirements are managed by the General Support System rather than the EaaS system, but EaaS will synchronize with Active Directory and may maintain this information. This information typically includes User Principal Name, first, middle, and last name, organization, office number, email address and phone number.

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: The HHS Email as a Service System (EaaS) is a Major Application (MA) supporting the transfer of messages among users of the system; messages can be sent from HHS staff members to other HHS staff members or externally to other e-mail users; that is to say, this e-mail system will have all the capabilities expected of other e-mail systems. Data processed on the EaaS is considered Controlled Unclassified Information (CUI).

EaaS stores or passes PII data that could be contained in e-mails between individual users sending and receiving e-mails on the system. Those e-mails would be stored on a service provider's cloud servers. Users would also have the ability to save e-mails in local archives on their individual workstations.

In most cases, the submission of PII will be voluntary, but required in order to receive benefits, serve as an employee of HHS, etc. The nature of the data collection will vary widely along with the underlying business practice.

Note that under some analyses, the use of an e-mail service would be considered not to involve the collection, maintenance, use, or sharing of PII, but to be the use of a "common carrier" that merely transmits the PII in the service of other business practices and applications.

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.
Name: Checked True
E-Mail Address: Checked True
Phone Numbers: Checked True
Device Identifiers: Checked True
Q15 Other 1: Any information a user chooses to include in an email message that may contain unspecified PII data.
Q15 Other 3: Active Directory credential information (UID) to allow for mailbox synchronization and email delivery

Question 16 : Q6
Indicate the categories of individuals about whom PII is collected, maintained, or shared.
Employees: Checked True
Public Citizens: Checked True

Business Partner/Contacts (Federal/state/local agencies: Checked True
Vendor/Suppliers/Contractors: Checked True
Patients: Checked True
Q16 Other: Any information a user chooses to include in an email message that may contain unspecified PII data.

Question 17: How many individuals' PII is in the system?
Question 17 Answer: 1,000,000 or more

Question 18: For what purpose is PII used?
Question 18 Answer: The uses of PII would be as varied as the functions and activities of HHS. Uses could include determination of benefits; health care payment, treatment or operations; conduct of health-related research; internal administrative and human resources functions; conduct of background checks; disciplinary actions; certification of health care service providers; or any of dozens of other activities HHS conducts. Active Directory credential information (primarily User Principal Name, userID and authenticator) is used by the system for authentication purposes only.

The EaaS system may also access additional information stored in the General Support System's Active Directory such as electronic address information, but this information is defined by the GSS, and not needed by the EaaS system.

Question 19: Describe secondary uses for which PII will be used (e.g. testing, training or research)
Question 19 Answer: No root-level or administrative users will have access to all the PII in this system. It is conceivable that HHS will employ some form of data loss prevention or discovery tool to identify PII contained in e-mails for purposes of complying with a discovery request or evaluating its privacy and security practices.

Question 20: Describe the function of the SSN.
Question 20 Answer: Not Applicable. However, SSNs may be transmitted in individual e-mails, but not according to any particular, defined use and would be subject to HHS encryption policy.

Question 20A: Describe the function of the SSN.
Question 20A Answer: Not Applicable

Question 21: Describe secondary uses for which PII will be used (e.g. testing, training or research)
Question 21 Answer: Not Applicable. Information use and disclosure over this system is governed by the laws and regulations of the individual business practice that this system is used to conduct.

Question 22: Describe secondary uses for which PII will be used (e.g. testing, training or research)
Question 22 Answer: No

Question 23A: Identify the OMB information collection approval
number and expiration date
Question 23A Answer: Not Applicable

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
Hard Copy: Mail/Fax: Checked True
Email: Checked True
Online: Checked True
Other: Checked True
Government Sources
Within the OPDIV: Checked True

Other HHS OPDIV: Checked True
State/Local/Tribal: Checked True
Foreign: Checked True
Other Federal Entities: Checked True
Other: Checked True
Non-Government Sources
Members of the Public: Checked True
Commercial Data Broker: Checked True
Public Media/Internet: Checked True
Private Sector: Checked True
Other: Checked True

Question 24: Is the PII shared with other organizations?
Question 24 Answer: Yes

Question 24A : Identify with whom the PII is shared or disclosed and for what purpose.
Identify with whom the PII is shared or disclosed and for what prupose.
Within HHS: Checked True
Identify with whom the PII is shared or disclosed and for what prupose.
Within HHS: email address shared as part of normal communication. Content of email varies with business function
OtherFed: Checked True
OtherFed: email address shared as part of normal communication. Content of email varies with business function
OtherFed: Checked True
OtherFed: email address shared as part of normal communication. Content of email varies with business function
OtherFed: Checked True
OtherFed: email address shared as part of normal communication. Content of email varies with business function

Question 24B: Describe any agreements in place that autorizes the information sharing.
Question 24B Answer: The agreements governing information exchange will vary with the business functions and purposes of exchanging e-mail. Memorandum of Understanding and Information Sharing Agreements are used between EaaS and CMS.

Question 24C: Describe any agreements in place that autorizes the information sharing.
Question 24C Answer: The HHS EaaS may be required to make such disclosures in the event that discovery is required pursuant to a legal action; at the request of the Secretary; if needed to respond to public health or other national emergencies; or to investigate privacy or security breaches.   Such requests can be performed by an approved System Administrator through the use of a mail query function submitted via the system interface portal., which allows for mailbox searches based on predefined criteria.

An accounting of responses for such disclosures is managed through the existing management processes within HHS/OS.

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: The processes will vary along with the underlying business processes and practices that the use of e-mail is supporting.

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

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: No PII data is specifically collected or used through the use of an e-mail system; therefore, there are no notifications to users about PII data and no consent obtained from individuals. Obtaining consent and/or providing notification is part of the business processes underlying the use of an e-mail service.

Any PII data contained in e-mail messages is only shared with the user(s) to whom the e-mail is sent.

Question 28: Describe the process to notify and maintain consent from the individuals whose PII is in the system.
Question 28 Answer: No PII data is specifically collected or used through the use of an e-mail system; therefore, there are no notifications to users about PII data and no consent obtained from individuals. Obtaining consent and/or providing notification is part of the business processes underlying the use of an e-mail service.

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: There is a Department-wide process. Individuals would not be likely to discover concerns through the use of PII in the e-mail system, but through the underlying business processes. Avenues for redress would include contacting the operations centers, help desks or customer service providers of those individual business operations. Members of the public could also avail themselves of the Freedom of Information Act (FOIA) or Privacy Act redress services.

For issues with PII detected by HHS staff members, individuals could also report suspected fraud, breaches, or other issues to the Computer Security Incident Response Center (CSIRC) or to the business process owner.

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: Data integrity is maintained at the level of the business process, or through maintenance of the applications that support business processes. Review of PII in e-mail systems would not be efficient or appropriate. Email message headers and attachments may be reviewed and sorted through the use of predefined search options, including key-word search, to support security incident response, data loss prevention, or e-discovery.

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 retrieve and use e-mail messages for day to day work functions.
Administrators Check Box: Checked True
Administrator Reason: To operate and maintain the e-mail system
Contractors Check Box: Checked True
Contractors Reason: Specifically authorized contractors serving as System Administrators will have access to Active Directory credential information for performing synchronization and testing duties required in the normal operation of the system.

Question 32: Describe the procedures in place to determine which system users (administrators, developers,
contractors, etc.) may access PII
Question 32 Answer: Only users (i.e., those authorized to send and receive e-mails) and administrators are able to access the contents of e-mails. The cloud service providers will be prevented from accessing contents of e-mails using encryption standards, and accessing the content will not be part of the services provided.

HHS employees and contractors that have completed the personnel screening process and corresponding forms and documents are provided email accounts as part of their employment package, and these mail accounts are accessed through EaaS. EaaS Administrators are approved by the Program Manager, and must complete necessary Network Access Request forms and training to obtain the elevated privileges required for administrative duties. The EaaS administrator must also register and request access, and sign corresponding NDAs, to the Microsoft Administration Portal for access to the management interface for the cloud-based components.

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: This is a standard e-mail system, and e-mails are sent from user to specified recipients. Other parties (system administrators, contractors, users not party to a specific communication, etc.) will not have access to e-mails not specifically addressed to them. Cloud providers in particular are not expected to have any access to the content of transmissions.

HHS EaaS system administrators with the appropriate permissions, who have signed Rules of Behavior and performed the required training, are able to access the contents of e-mails, for authorized purposes such as e-discovery or detection of breaches.

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: All users are required to complete annual Information Security Training and Privacy Awareness Training.

Question 35: Describe training system users receive (above and beyond general security and privacy awareness
training).
Question 35 Answer: User will be provided training regarding the basic concepts of accessing email and collaboration services offered by the EaaS cloud-based solution. EaaS Administrators are required to complete training in Security Incident Response, Contingency Planning and Operations, and Role-Based training.

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: User can archive messages containing PII data on their workstation or in their mailbox indefinitely. Otherwise, the data retention policy on the storage arrays is 14 days. If a user deletes a message, at which time it is moved to the Deleted Items Recovery folder for 14 days. After this period, the deleted mail is stored in a purge folder for 14 days, during which time only authorized administrators can access it.

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: EaaS implements security controls to protect PII, as defined by OMB mandates, the Federal Information Security Management Act (FISMA), and NIST Special Publications (SP) 800-53, 800-37, 800-122, NIST Federal Information Processing Standards (FIPS) 200, 201, 199, 197, 140-2, and other associated documents as outlined by Federal Risk and Authorization Management Program (FedRAMP)

(www.fedramp.gov). This includes achieving and maintaining an Authority to Operate (ATO)

PII will be secured within the system through the use of administrative controls in the form of:
- Mandatory security awareness and privacy training for all users
- Role-based training for privileged users.
- Personnel screening as required by HHS,
- Completion of contractual agreements and Rules of Behavior.
- Users can encrypt email traffic, including those containing PII, in accordance with applicable HHS policies.

Technical controls include:
- Role-based access controls based on Active Directory permissions to obtain authorized access to the system. All user login will be logged, with auditing performed as part of the EaaS Continuous Monitoring program.
- Spam and email content filtering
- Anti-malware software installed on EaaS servers
- FIPS 140-2 compliant encryption of data in transit
- Restricted access to the GCC through the HHS Trusted Internet Connection (TIC) Access Points
- Information Flow Control through the use of firewalls, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Security Information and Event Management (SIEM), Data Loss Prevention (DLP) and Continuous Data Protection (CDP) policy that allows for direct remote OpDiv administration
- Non-repudiation through support of digital signatures and encrypted email, using PIV and other types of digital certificates.

Physical controls include:
- Hosting within data centers which control and monitor physical access to the system components, including visitor control and auditing of access records
- Protection of power equipment and cabling, transmission medium, output devices and use of emergency power and shutoff systems as well as fire and water damage protection.