Status: Final

Form Date: 14-MAY-14

Question 1: OPDIV
Question 1 Answer: OS

Question 2: PIA Unique Identifier (UID):
Question 2 Answer: P-7988940-281745

Question 2A: Name:
Question 2A Answer: Malware Virtualization Compartmentalization

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: Initiation

Question 3B: Is this a FISMA Reportable System?
Question 3B Answer: No

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

Question 5: Identify the operator
Question 5 Answer: Agency

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: 15-MAY-14

Question 11: Describe the purpose of the system.
Question 11 Answer: This system provides malware compartmentalization capabilities. Malware is is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Invincea and Bromium are endpoint security tools that will be piloted enterprise wide. This pilot program will cover separate installations of both Bromium and Invincea Management Servers at each of the following Operational Divisions:
• CSO- Cyber Security Operations
• CDC- Center for Disease Control
• CMS- Centers for Medicare & Medicaid Services
• OIG- Office of Inspector General
• NIH- National Institutes of Health
• FDA- Food and Drug Administration

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: Log Data
Malware and Threat Data

User activities in relation to malware

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: Management Server collecting endpoint information on user machines. System will generate log data and malware and threat analysis data, permanently for the duration of the pilot.

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: Not Checked
Employment Status: Not Checked
Q15 Other 1: malware related web activities

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

Question 17: How many individuals' PII is in the system?
Question 17 Answer: <100

Question 18: For what purpose is PII used?
Question 18 Answer: Primary purpose of PII being used is for forensic investigation of malware. For user authentication
its use will be the same as any information collected by firewalls and proxies such as IP addresses, ports and protocols. Its use is solely for incident attribution and tracking to resolution.

Question 19: Describe secondary uses for which PII will be used (e.g. testing, training or research)
Question 19 Answer: Secondary uses for use of PII will be for research into the pilot products.

Question 20: Describe the function of the SSN.
Question 20 Answer: N/A

Question 20A: Describe the function of the SSN.
Question 20A Answer: N/A

Question 21: Describe secondary uses for which PII will be used (e.g. testing, training or research)
Question 21 Answer: Governing legal authority is FISMA, 44 U.S.C. 3541

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

Question 23 : Identify the sources of PII in the system.
Email: Not Checked
Government Sources
Within the OPDIV: Checked True
Other HHS OPDIV: Checked True

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: All systems with the software installed will be subject to the standard system use notification at log on.

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: Security tool installed on the system to monitor system activities.

Question 28: Describe the process to notify and maintain consent from the individuals whose PII is in the system.
Question 28 Answer: Users are all federal IT users who agreed to data collection as part of their federal IT Rules of Behavior.

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: Users are all federal IT users who agreed to data collection as part of their federal IT Rules of Behavior.

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: During this limited pilot there is no plan or process for further review.

Question 31 : Identify who will have access to the PII in the system and the reason why they require access.
Administrators Check Box: Checked True
Administrator Reason: Review of security logs

Question 32: Describe the procedures in place to determine which system users (administrators, developers,
contractors, etc.) may access PII
Question 32 Answer: Administrators, managers responsible for network operations, will be able to access PII, users will not.

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: There are no further restrictions. Administrators have access to all security log information within the system. The system only records user activities with regards to malware activity.

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 have participated in system demo's for awareness and training purposes.

Question 35: Describe training system users receive (above and beyond general security and privacy awareness
training).
Question 35 Answer: N/A

Question 36: Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to
privacy provisions and practices.
Question 36 Answer: No

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: The system will be decommissioned at the end of the pilot, all information will be destroyed. Estimated end of pilot date: June 9, 2014

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: Only system administrators can log into the system as well as protected by network boundary.

Question 39: Identify the publicly-available URL:
Question 39 Answer: N/A