and mitigate zero day malware exploits. In short, PII could be included within a particular malware package, exploit or exfiltration attempt passing through a network boundary device, where the SHARKSHADOW IS has been deployed. In the before described scenario, PII would be collected. All PII information is transported over encrypted IPSEC tunnels and placed into an automated virtual machine to be tested for the presence of malware. Once analysis is completed, the VM may create a custom signature file for the malware identified, and that is the only information removed from the virtual machine. All other data is destroyed.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

□ Privacy Act Statement □ Privacy Advisory ☒ Not Applicable

PII is not intentionally collected.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

☒	Within the DoD Component	Specify. DISA Global Operations Center
□	Other DoD Components	Specify.
☒	Other Federal Agencies	Specify. National Security Agency & Joint Special Operations Command
□	State and Local Agencies	Specify.
□	Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.
□	Other *(e.g., commercial providers, colleges).*	Specify.

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

□ Individuals

☒ Existing DoD Information Systems

□ Other Federal Information Systems

□ Databases

□ Commercial Systems

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

☒ E-mail

□ Face-to-Face Contact

☒ Fax

☒ Information Sharing - System to System

☒ Other *(If Other, enter the information in the box below)*

□ Official Form (*Enter Form Number(s) in the box below)*

□ Paper

□ Telephone Interview

□ Website/E-Form

PII is not intentionally collected within the SHARKSHADOW system. Rather, it is merely a possibility that PII may be contained within various Internet traffic that is being captured and processed by the SHARKSHADOW information system, as the system attempts to detect and mitigate zero day malware exploits. In short, PII could be included within a particular malware package, exploit or exfiltration attempt passing through a network boundary device, where the SHARKSHADOW IS has been deployed. In the before described scenario, PII would be collected. All PII information is transported over encrypted IPSEC tunnels and placed into an automated virtual machine to be tested for the presence of malware. Once analysis is completed, the VM may create a custom signature file for the malware identified, and that is the only information removed from the virtual machine. All other data is destroyed.

k. Does this DoD Information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information must be consistent.

□ Yes ☒ No

If "Yes," enter SORN System Identifier

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

PII is not intentionally collected within the SHARKSHADOW system. Rather, it is merely a possibility that PII may be contained within various Internet traffic that is being captured and processed by the SHARKSHADOW information system, as the system attempts to detect and mitigate zero day malware exploits. In short, PII could be included within a particular malware package, exploit or exfiltration attempt passing through a network boundary device, where the SHARKSHADOW IS has been deployed. In the before described scenario, PII would be collected. All PII information is transported over encrypted IPSEC tunnels and placed into an automated virtual machine to be tested for the presence of malware. Once analysis is completed, the VM may create a custom signature file for the malware identified, and that is the only information removed from the virtual machine. All other data is destroyed.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. GRS 3.1, Item 051

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

The system does not store PII in a database. Any PII that is captured would be destroyed after the virtual machines perform analysis.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply).

(a) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) If direct or indirect authority does not exist, DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component must be identified.

DoD Directive 5105.19, Defense Information Systems Agency (DISA).

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (OMB) Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information. This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

□ Yes ☒ No □ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

OMB approval is not required since the WHS IC Management Office has determined that this PIA does not require an OMB Control Number, since the public does not log into the system.