PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

CrowdStrike Falcon Platform

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

02/26/2026

Cloud Broker Service

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)*

- ☐ From members of the general public
- ☐ From Federal employees
- ☒ from both members of the general public and Federal employees
- ☐ Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one.)*

- ☐ New DoD Information System
- ☐ New Electronic Collection
- ☒ Existing DoD Information System
- ☐ Existing Electronic Collection
- ☐ Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

CrowdStrike provides a comprehensive and fully scalable security platform that can protect customers' endpoints and cloud workloads with a full suite of modules that offer in-depth protection. Falcon Platform consists of two (2) key components. Each component has been analyzed to determine if any elements of that component collect and/or store PII. The type of PII collected and/or stored by Falcon Agent. Both components store PII. For the Falcon Sensor PII appearing in machine event fields, such as user names, machine names, or PII the customer may include in file names or file submissions. For the Falcon Cloud. PII appearing in machine event fields, such as user names, machine names, or PII the customer may include in file names or PII the customer may include in file names or file submissions. PII may include numerous types of PII including employee and beneficiary contact information, military information and demographic information.

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

Machine event data is monitored to detect, prevent, and respond to cybersecurity attacks. Machine event data may include user account, computer name, host name, and other system identifiers as well as file names and file paths. Consequently, PII may be collected to the extent that it exists in a collected field or file submission. Data collected by the sensor is sent to the cloud as described above as part of the SaaS-based cybersecurity offering.

e. Do individuals have the opportunity to object to the collection of their PII? ☐ Yes ☒ No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

Individuals do not have the opportunity to object to the collection of their PII because this system is not the initial point of collection; however, the source system may provide the individual the opportunity to object to the collection.

f. Do individuals have the opportunity to consent to the specific uses of their PII? ☐ Yes ☒ No

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

Individuals do not have the opportunity to object to the collection of their PII because this system is not the initial point of collection; however, the source system may provide the individual the opportunity to object to the collection.

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

This system is not the initial collection point for the PII. The PII is obtained from an existing DoD information system or electronic collection, therefore no Privacy Act Statement or Privacy Advisory is required.

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

☒	Within the DoD Component	Specify.	Defense Health Agency
☐	Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	
☐	Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	
☐	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	☐	Databases
☒	Existing DoD Information Systems	☐	Commercial Systems
☐	Other Federal Information Systems		

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

☐	E-mail	☐	Official Form (*Enter Form Number(s) in the box below)*
☐	In-Person Contact	☐	Paper
☐	Fax	☐	Telephone Interview
☒	Information Sharing - System to System	☐	Website/E-Form
☐	Other *(If Other, enter the information in the box below)*		

Via the Falcon Sensor and Falcon Cloud.

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.

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.

1606-17: GRS 3.2, item 036
1105-06: DAA-0330-2015-0005-0002
1105-07: DAA-0330-2015-0005-0003

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

(3) Retention Instructions.

FILE NUMBER: 1606-17
FILE TITLE: Cybersecurity Event Logs
DISPOSITION: Temporary. Cut off monthly. Destroy 30 months after cutoff.

FILE NUMBER: 1105-06
FILE TITLE: Cybersecurity Assessments
DISPOSITION: Temporary. Cut off annually. Destroy 10 years after cutoff.

FILE NUMBER: 1105-07
FILE TITLE: Cyber Incident Response and Analysis
DISPOSITION: Temporary. Cut off annually. Destroy 10 years after cutoff.

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.

5 USC 301, Departmental Regulations; 10 USC 142, Chief Information Officer; 40 USC 11315, Agency Chief Information Officer; 44 USC 3506, Federal Agency Responsibilities; 44 USC § 3554, Federal Agency Responsibilities; Public Law 104-191, Health Insurance Portability and Accountability Act of 1996; 10 USC, Ch. 55, Medical and Dental Care; 10 USC 1073c, Administration of Defense Health Agency and Military Medical Treatment Facilities; and DoD Manual 6025.18, Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs.

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.

The information collected within this system is for correlating security information and providing dashboards system to system (the system components, applications, or electronic collections within) in accordance with DoDM 8910.01, Volume 2, Enclosure 3, paragraph 8b(5).