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:

Joint Incident Management System (JIMS)

2. DOD COMPONENT NAME:

Defense Information Systems Agency

3. PIA APPROVAL DATE:
1/31/2023

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.

The JIMS is a DoD network defense incident handling application designed to capture all information assurance related to cyber incidents in the department. JIMS ensures timely flow of crucial network intelligence across the DoD/U.S. Government and ally boundaries to reflect the collective reporting of adversary actions, intentions, and capabilities to assist in shaping tactical, strategic, and military response strategies. The types of personal information about individuals that could be collected include names, email, personal email, DoD ID, and any information related to an incident.

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)*

Mission and administrative related use. A user has the ability to add comments that may include PII during incident entry. The personal information in the JIMS system is captured as part of incident information.

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.

PII in the JIMS system is captured as part of the incident information.

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.

PII in the JIMS system is captured as part of the incident information.

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

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

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. DISA

☒ Other DoD Components *(i.e. Army, Navy, Air Force)* — Specify.
C5ISR "Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance, and Reconnaissance.
DARPA Defense Advanced Research Projects Agency
DAU Defense Acquisition University
DCAA Defense Contract Audit Agency
DCMA Defense Contract Management Agency
DCSA Defense Counterintelligence and Security Agency
DECA Defense Commissary Agency
DFAS Defense Finance and Accounting Service
DHA Defense Health Agency
DIA Defense Intelligence Agency
DISA Defense Information Systems Agency
DLA Defense Logistics Agency
DLSA Defense Legal Services Agency
DMA Defense Media Activity
DMEA Defense Microelectronics Activity
DoDEA DoD Education Activity
DoDHRA Defense Human Resources Activity
DoDIG Department of Defense Inspector General
DoDTRMC DoD Test Resource Management Center
DPAA Defense POW/MIA Accounting Agency
DREN Defense Research Engineering Network
DSCA Defense Security Cooperation Agency
DSS Defense Security Service
DTIC Defense Technical Information Center
DTRA Defense Threat Reduction Agency
DTSA Defense Technology Security Administration
HPCMP High Performance Computing Modernization Program

☒ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)* — Specify.
JCS Joint Chiefs of Staff
JFHQ-DODIN JOINT FORCE HEADQUARTERS–DOD INFORMATION NETWORK
PFPA Pentagon Force Protection Agency
SDC Secretary of Defense Communications
SPAWAR Space and Naval Warfare
USAFRICOM United States Africa Command
USCENTCOM United States Central Command
USCYBERCOM United States Cyber Command
USEUCOM United States European Command
USPACOM United States Pacific Command
USNORTHCOM United States North Command
USSOCOM United States Special Operations Command

☒ State and Local Agencies

Specify. USSOUTHCOM United States South Command
USSPACECOM United States Space Command
USSTRATCOM United States Strategic Command
USTRANSCOM United States Transportation Command
WHS Washington Headquarters Services
JS Joint Staff
JSP Joint Service Provider
MDA Missile Defense Agency
NDU National Defense University
NGA National Geospatial-Intelligence Agency
NIWC Naval information warfare Center
NRO National Reconnaissance Office
OEA Office of Economic Adjustment
OSD Office of the Secretary of Defense
DOC Department of Commerce
DOE Department of Energy
DOJ Department of Justice
DOS Department of State
USMC United States Marine Corp
USN United States Navy
USA United States Army
USAF United States Air Force
USCG United States Coast Guard
NSA National Security Agency/Central Security Service

☐ 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
☐ In-Person 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

Entered directly into JIMS or by a feed from an existing system.

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 DUSDI 01-DoD

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. GRS 3.2 item 20

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

(3) Retention Instructions.

(DAA-GRS-2013-0006-0002) Temporary. Destroy 3 year(s) after all necessary follow-up actions have been completed, but longer retention is authorized if required for business use.

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.

The following authority allows Joint Incident Management System (JIMS) to collect the following data:
10 U.S.C. 137, Under Secretary of Defense for Intelligence; 44 U.S.C. 3554, Federal agency responsibilities; 44 U.S.C. 3557, National security systems; Public Law 112-81, Section 922, National Defense Authorization Act for Fiscal Year 2012 (NDAA for FY12), Insider Threat Detection (10 U.S.C. 2224 note); Public Law 113-66, Section 907(c)(4)(H) (NDAA for FY14), Personnel security (10 U.S.C. 1564 note); Public Law 114-92, Section 1086 (NDAA for FY16), Reform and improvement of personnel security, insider threat detection and prevention, and physical security (10 U.S.C. 1564 note); Public Law 114-328, Section 951 (NDAA for FY17), Enhanced security programs for Department of Defense personnel and innovation initiatives (10 U.S.C. 1564 note);National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs; and DoD Directive 5205.16, The DoD Insider Threat Program; DoD Instruction 5205.83, DoD Insider Threat Management and Analysis Center (DITMAC)

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 Control Number: 0704-0478; Expiration Date: None