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:

Enterprise Information Technology as a Service (EITAAS Wave 1)

2. DOD COMPONENT NAME:

United States Air Force

3. PIA APPROVAL DATE:

06/05/2025

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
- [x] 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
- [x] 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.

EITAAS WAVE 1 :
EITSM:
EITSM leverages the ServiceNow SaaS solution to provide an Enterprise IT Service Management capability (E-ITSM). Information technology service management (ITSM) are activities performed by an organization to design, build, deliver, operate and control information technology (IT) services offered to customers. The system is located in an Azure IL5 cloud and is accessible through a DISA BCAP. EITSM Wave 1 NIPR effort will conduct help desk operations as part of the Enterprise Information Technology Service Management (EITSM) requirement, agents will collect PII elements, typically referred to as “ROLODEX PII, business PII, office PII or non-sensitive PII” including the following data types:

1. Home/Cell Phone 2. Official Duty Address 3. Work E-mail address 4. Financial Information 5. Official Duty Telephone Phone 6. Position/ Title 7. Rank/Grade 8. DoD ID Number 9. Name(s) 10. Assigned MAJCOM 11. Assigned Unit 12. Assigned Unit Location 13. Assigned Unit Street 14. Assigned Unit Zip Code 15. Attached MAJCOM 16. Attached Unit 17. Attached Unit Location 18. Attached Unit Name 19. Building 20. Category 21. Common name (cn) 22. Distinguished Name (dn) 23. Enterprise User Name 24. Federated Assured Personal Identifier (fapi) 25. Mail address 26. Mobile Phone 27. Parent Unit Name 28. Projected Unit 29. Projected Unit Date 30. Room 31. Service Branch 32. Last Name (sn) 33. Login name 34. Work contact information 35. Administrative organization 36. Duty organization 37. Department

IT STOREFRONT: .
The IT Storefront leverages the service catalog functionality within the Wave 1 ServiceNow EITSM system. Specifically, the storefront includes a “front end” portal accessible to Airmen and Guardians to initiate and track order requests and “back end” workflows to manage approvals and order fulfillment. The storefront currently includes one capability, allowing MAJCOMs and bases to order field services from the Wave 1 vendor. The storefront road-map includes on-boarding additional capabilities, allowing Airmen and Guardians to order an increasingly wide array of hardware, software, and IT services. The IT Storefront will collect the following financial information data types:

1.Credit Card Number 2.Credit Card Expiration Date 3.Credit card Security Code 4.Card Holders name 5.Card Holders commercial phone number 6.Card Holder email 7.Card Holder's Billing Address.
This information will be held in Service now until the purchased product is processed and shipped.

CAMM:
Cyber Asset Metadata Management (CAMM) leverages the Axonius platform to provide comprehensive visibility and actionability across cyber assets, SaaS applications, software, identities, exposures, and infrastructure for asset within EITaaS Wave 1 for tracking Information Technology assets. All collected data will remain on Government Furnished Equipment (GFE) and will be encrypted if stored.

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)*

Wave 1 NIPR PII elements will be used for verification and validation of user's identity against existing AF Active Directory for users being served by the EITSM system. Data collected is required for tracking of service tickets, without the information, resolution tracking would be impossible and technicians would not be able to support subsequent interactions with user's open tickets in the EITSM system.

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.

Wave 1 NIPR PII data utilized is derived from an existing system (Air Force Identity(AFID) Management; eMASS; DAF ICAM) and used to identify individuals requesting service support. Users can deny providing any PII data at the beginning of the service or help-desk ticket creation but will be prompted to provide information in order for the service desk to identify and contact them. Credit Card information will be collected only after consenting via a Privacy Act Statement popup box.

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.

Wave 1 NIPR PII data utilized is derived from an existing system (Air Force Identity(AFID) Management; eMASS; DAF ICAM) and used to identify individuals requesting service support. Data collected is required for tracking of service tickets, without the information resolution tracking would be extremely difficult and technicians would not be able to follow up on open tickets in the EITSM system. Credit Card information will be collected only after consenting via a Privacy Act Statement popup box.

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

SORN: DoD 0015
Authority:
Title 10 United States Code (U.S.C.) 9013, Secretary of the Air Force; 5 U.S.C. 301, Departmental Regulation; DoD Directive 5105.19, Defense Information Systems Agency (DISA); Privacy Act Information: information accessed through this system must be protected in accordance with the Privacy Act of 1974, as amended, and AFI 33-332;

Purpose: The purpose of the data is for use in desktop support, and technical support of information systems.
Routine Uses: Data will not be used outside of the DoD
Disclosure: Voluntary, omitting some requested information will delay corrective actions for the requester.

A. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal government when necessary to accomplish an agency function related to this system of records. B. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature. C. To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent. D. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding. E. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.
F. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record. G. To appropriate agencies, entities, and persons when (1) the DoD suspects or confirms a breach of the system of records; (2) the DoD determines as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm. H. To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach. I. To another Federal, State or local agency for the purpose of comparing to the agency's system of records or to non-Federal records, in coordination with an Office of Inspector General in conducting an audit, investigation, inspection, evaluation, or some other review as authorized by the Inspector General Act of 1987, as amended. J. To such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.

ServiceNow Website: https://servicecenter.af.mil/
Banner:
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.
NOTICE: There is the potential that information presented and exported from the AF Portal contains FOUO or Controlled Unclassified Information (CUI). It is the responsibility of all users to ensure information extracted from the AF Portal is appropriately marked and properly safeguarded. If you are not sure of the safeguards necessary for the information, contact your functional lead or Information Security Officer.
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.

Website: https://www.my.af.mil/afp/netstorage/login_page_files_cloud_one/dod-user-agreement.html
Banner:
DOD User Agreement
By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:
You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government-authorized use only.
You consent to the following conditions:
The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
At any time, the U.S. Government may inspect and seize data stored on this information system.
Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.
This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.
Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:
Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.
The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.
Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.
Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.
A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.
These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.
In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law

enforcement, or counterintelligence investigative searching, (ie., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.
All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.
Last Modified: 9 DECEMBER 2021

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.	DAF, Space Force
☐ 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.	CACI, Inc.- Federal, FA8726-22-A-0001; EXP: 29 Aug 2027, CACI GSA contract has the 52.224-1, 52.224-2 and 52.224-3 and 52.239-1 - https://gsaelibrary.gsa.gov/ElibMain/home.dohttp:/www.gsaelibrary.gsa.gov/ElibMain/contractClauses.do?scheduleNumber=MAS&contractNumber=47QSEA19D00A9&contractorName=CACI%2C+INC.+-+FEDERAL&duns=N3PBJAVNKF61&listFor=C&view=clauses
☐ 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

Existing DOD Information systems: Data will be derived from - Air Force Identity(AFID) Management; eMASS; DAF ICAM;Enterprise Application and Services Forest (EASF)

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)*

System to System:
Data will be derived from - Air Force Identity(AFID) Management; eMASS; DAF ICAM; Enterprise Application and Services Forest (EASF); WEBSITE: https://eitaas.servicecenter.af.mil/

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 DoD 0015

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. DAA-GRS-2013-0005-0004

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

(3) Retention Instructions.

Destroy 3 year(s) after agreement, control measures, or procedures are superseded or terminated; or records have no outstanding payment issues; or project/activity/transaction is obsolete, completed, or superseded, whichever is appropriate

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.

Title 10 United States Code (U.S.C.) 9013, Secretary of the Air Force; 5 U.S.C. 301, Departmental Regulation; DoD Directive 5105.19, Defense Information Systems Agency (DISA); Privacy Act Information: information accessed through this system must be protected in accordance with the Privacy Act of 1974, as amended, and AFI 33-332.

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.

Neither the help desk information collection or any other part of the system is subject to the PRA per WHS.