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:

Collaboration Pathfinder With Cloud Service Provider (CSP) -- (CHES/AF Office 365 SaaS Cloud System)

2. DOD COMPONENT NAME:

United States Air Force

3. PIA APPROVAL DATE:

04/20/20

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

- [ ] From members of the general public
- [ ] From Federal employees and/or Federal contractors
- [x] From both members of the general public and Federal employees and/or Federal contractors
- [ ] 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.

The unclassified Air Force (AF) Office 365 SaaS Cloud system provides a consolidated environment for authorized AF users with CAC for the purpose of collaboration and content management needs. The AF Office 365 SaaS Cloud system is an integrated service covered by the Collaboration Pathfinder With Cloud Service Provider (CSP) ATO.

The AF Office 365 system provides messaging, collaboration, productivity, and content management to support and bring value to Airmen executing missions agnostic of device and location. This system ultimately delivers the office anywhere experience through an integrated strategy that improves services, enhances productivity, and increases mobility while reducing cost.

PII Collected: Since PII collection is not under the control of the Office 365 Program Office but under the AF entity collecting source, it is not possible for the Program Office to definitively identify what is collected.

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-related use and administrative use as determined by each Air Force entity collecting the data.

e. Do individuals have the opportunity to object to the collection of their PII? [ ] Yes [x] 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.

The AF Office 365 system is approved for the transfer and storage of UNCLASSIFED files in any format to include FOUO, controlled unclassified information (CUI) which may contain PII that may have been collected via another method (i.e. another source). The AF entity collecting PII is responsible for ensuring owners of the PII have the opportunity to object to the collection of their PII and that all requirements regarding notification and consent have been complied with prior to the PII being introduced in to any AF Office 365 application/environment.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [ ] Yes [x] 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.

The AF Office 365 system is approved for the transfer and storage of UNCLASSIFED files in any format to include FOUO, controlled unclassified information (CUI) which may contain PII that may have been collected via another method (i.e. another source). The AF entity collecting PII is responsible for ensuring owners of the PII have the opportunity to object to the collection of their PII and that all

requirements regarding notification and consent have been complied with prior to the PII being introduced in to any AF Office 365 application/environment.

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 is the responsibility of the collecting AF entity.

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.	This is the responsibility of the collecting AF entity.
☒	Other DoD Components	Specify.	This is the responsibility of the collecting AF entity.
☒	Other Federal Agencies	Specify.	This is the responsibility of the collecting AF entity.
☒	State and Local Agencies	Specify.	This is the responsibility of the collecting AF entity.
☒	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.	This is the responsibility of the collecting AF entity.
☒	Other *(e.g., commercial providers, colleges).*	Specify.	This is the responsibility of the collecting AF entity.

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

This is the responsibility of the collecting AF entity.

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)*

☒ Face-to-Face Contact ☒ Paper

☒ Fax ☒ Telephone Interview

☒ Information Sharing - System to System ☒ Website/E-Form

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

This is the responsibility of the collecting AF entity.

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.

AF Office 365 is not a system of record and is only approved for file and information sharing and collaboration. Users will not retrieve information by name or unique identifier.

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. T &R 33 - 45 R 04.00/DAA-GRS-2013-0002-0016; T&R 33 - 42 R 02.00/

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

(3) Retention Instructions.

T 33 - 45 R 04.00: Electronically Stored Information (ESI) Project Control & Support Background, Working Papers, Draft Documents - Destroy or delete when 2 years old, or 2 years after the date of the latest change, whichever is applicable

T 33 - 42 R 02.00 General Correspondence (Temporary), General Correspondence (Temporary) Duplicate Files - Destroy after 1 year

National Archives and Records Administration (NARA) General Records Schedule 5.1 Item 020: Non-recordkeeping copies of electronic records - Destroy immediately after copying to a recordkeeping system or otherwise preserving, but longer retention is authorized if required for business use.

Note 1: Among the NARA dispositions cited in this field, the one with the longest retention time will be used on the system's records data. If dispositions provided do not correspond/correlate to your specific record, please refer to the Air Force Records Disposition Schedule located in AFRIMS to find the appropriate retention/disposition instructions.

Note 2: Transfer finalized official records/documents to the relevant Electronic Record Keeping System (inventory of records, IT system, case file, etc.), and apply the appropriate records disposition schedule.

Note 3: Review file(s) annually to determine if the file(s) merit continuing disposition; if not, dispose.

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.

This is the responsibility of the collecting AF entity. Some possible answers include the following. Pub. L. 106-229, Electronic Signatures in Global and National Commerce; OASD (C3I) Policy Memorandum, subject: DOD Digital Modernization Strategy dated 12 Jul 2019; OASD (C3I) Memorandum, subject: Common Access Card (CAC); 10 U.S.C. 9013, Secretary of the Air Force: powers and duties; DoD Instruction (DoDI) 5205.13, Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities; DoDI 8500.01, Cybersecurity; DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT); DoDI 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling; DoDI 8540.01, Cross Domain (CD) Policy; DoDI 8520.03, Identity Authentication for Information Systems; DoDI 8530.01, Cybersecurity Activities Support to DoD Information Network Operations; DoDI 8551.01, Ports, Protocols, and Services Management (PPSM); DoDI 8580.1, Information Assurance (IA) in the Defense Acquisition System; DoDI 8581.01, Information Assurance (IA) Policy for Space Systems Used by the Department of Defense; DoDI 8582.01, Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information; AFMAN 17-1203_AFGM2019-01, Information Technology (IT) Asset Management (ITAM); AF Instruction (AFI) 17-101, Risk management Framework (RMF) for Air Force Information Technology; and AFI 33-200, Air Force Cybersecurity Program Management; AFI 33-332, AF Privacy and Civil Liberties; AFI 33-322, AF Records Management, AFMAN 33-396, Knowledge Management.

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.

This is the responsibility of the collecting AF entity. The AF Office 365 system is approved for the transfer and storage of UNCLASSIFED files in any format to include FOUO, controlled unclassified information (CUI) which may contain PII that may have been collected via another method (i.e. another source).

NOTE: Sections 1 above is to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy. A Component may restrict the publication of Sections 1 if they contain information that would reveal sensitive information or raise security concerns.