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:

Marshall Center Network Office 365 (MCNET O365)

2. DOD COMPONENT NAME:

Defense Security Cooperation Agency

3. PIA APPROVAL DATE:

12/1/2025

George C. Marshall European Center for Security Studies (GCMC)

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 Marshall Center Microsoft Office 365 (MCNET O365) instance is a commercial IL2 cloud solution, fortified with IL4-level controls. It serves as the Software-as-a-Service (SaaS) extension of the Marshall Center Network (MCNET) infrasture. Both MCNET and MCNET O365 instance will support daily business operations at the George C. Marshall European Center for Security Studies (GCMC) in support of its partnership building mission which include, but not limited, to the following program services: Human Resources, Finance, Travel, Participant Affairs, Legal, Student Registrar, and Academic Instruction.

The information processed consists of staff work product and administrative data which by its nature also includes the use of various non-sensitive and sensitive personally identifiable information (PII). Note, this PIA will cover both MCNET and MCNET O365.

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)*

The intended use of the information collected is for mission-related and administrative uses as specified above. In addition, the PII is collected to manage various personnel actions to include the validation and reconciliation of travel orders, management of student/ participant activities, events and courses, in addition to certain PII that is used for identification purposes for access to DoD information and military installation.

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.

Employees implicitly consent to the capture and use of their PII at the time of employment for various personnel actions (e.g., Human Resources, training, security and travel, etc.) . Upon the collection of personal information, employees are provided appropriate Privacy Act Statements and given an opportunity to object to any collection of PII at that time.

Regarding members of the general public, participation in the international military education and training courses and opportunities at the GCMC is voluntary, and individuals may object to the collection of their PII upon request of the information. However, failure to provide the requested information may result in ineligibility of the training program opportunities and prevent access to US installation.

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.

Employees and other participants implicitly consent to the capture and use of their PII at the time of employment and participation in specific training program courses and opportunities, respectively.

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

Upon the collection of personal information, individuals subject to the Privacy Act are provided appropriate Privacy Act Statements. Access to the MCNET is mandatory before access to the MCNET 0365 instance. For access the DD Form 2875, System Authorization Access Request (SAAR) must be completed, and the form includes the following Privacy Act Statement:

Authority: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.

Purpose: To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.

Routine Use: None.

Disclosure: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

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.	DSCA Headquarters and Regional Centers and Fields Activities
☒ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	U.S. Army Garrison (Benelux, Stuttgart & Bavaria, Garmisch), DAI, DFAS and DTS
☒ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	Department of State (U.S. Embassies)
☐ 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.	Vectrus Inc. The contract contains provisions to ensure the confidentiality and security of PII are in place to to manage PII in the workplace, including language addressing the completion of initial and annual privacy training for contractor employees. Note, FAR Privacy Act clauses have been added to the contract.
☐ 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

MCNET

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)*

DD Form 2875, DD Form 1610, DA Form 31, DA Form 4187, DD Form1351-2, AE Form 600-77A, SF Form 182, and DD Form 577

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.

MCNET and MCNET-O365 are not systems of records for purposes of the Privacy Act, a SORN is not required to be published in the Federal Register.

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. See Below

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

(3) Retention Instructions.

FILE NUMBER: 101-01.1
FILE TITLE: Office Administrative Records
FILE DESCRIPTION: Records accumulated by individual offices that relate to routine day-to-day administration and management of the office rather than the mission-specific activities for which the office exists. Records include: • Staff locators, unofficial organizational charts, and office seating charts (see Exclusion 1) • Office-level administrative policies and procedures and files related to their development • Calendars or schedules of daily activities of non-high-level officials (see 212 for Senior-Level Officials) • Informal requests and tracking of personnel training, travel, supplies, and equipment, excluding procurement and payment records and forms requesting training (e.g., SF-182) • Internal office activity and workload reports • Studies and analyses of office administrative functions and activities • Non-mission related management reviews and surveys • Minutes of meetings related to administrative activities
DISPOSITION: Temporary. Cut off and destroy when business use ceases.
AUTHORITY: GRS 5.1, item 010 (DAA-GRS-2016-0016-0001)
PRIVACY ACT: Not applicable
FORMER FILE NUMBER(S): 101-01, 101-14, 101-15, 102-07, 103-14a, 923-02, 923-03, 1301-14, 1605-01, 1605-02

FILE NUMBER: 101-06
FILE TITLE: Records tracking and controlling access to protected information
FILE DESCRIPTION: Includes: • Records documenting receipt, internal routing, dispatch, or destruction of classified, and controlled unclassified information. • Tracking databases and other records used to manage overall program • Requests and authorizations for individuals to have access to classified and controlled unclassified records and information.
NOTE: Records documenting individuals' security clearances are covered under file numbers 202-40.1 and 202-40.4.
DISPOSITION: Temporary. Cut off after last form entry, reply, or submission; or when associated documents are declassified, decontrolled, or destroyed; or when an individual's authorization expires; whichever is appropriate. Destroy 2 years after cutoff.
AUTHORITY: GRS 4.2, item 030 (DAA-GRS-2019-0001-0002)
PRIVACY ACT: Not applicable
FORMER FILE NUMBER(s): 101-06, 101-09, 101-10, 101-11, 101-12, 101-18, 209-02, 209-03, 209-04, 20906, 704-04.4

FILE NUMBER: 1601-01
FILE TITLE: System Development Records

FILE DESCRIPTION: These records related to development of Information Technology (IT) systems and software applications through their initial stages up until hand-off to production which includes planning, requirements analysis, design, verification and testing, procurement, and installation. Records include case files containing documentation of planning, decision making, designing, programming, testing, evaluation, and problem solving. Includes records such as: • Project plans • Feasibility studies • Cost analyses • Requirements documents • Compliance documents including: o Privacy Threshold Analyses (PTAs) o Privacy Impact Assessments (PIAs) o Security Plan o Information Protection Plan • Change control records • Project Schedule • Plan of Action and Milestones (POA&M) • Configuration Management Plan • Resource Management Plan • Risk Assessment/Mitigation Plan • Security Plan • Disaster Recovery Plan • Test/ Acceptance Plan • Quality Control Plan • Deployment Guide • User Guide • Training Guide Exclusion: This item does not apply to system data or content.
NOTE: For certain technical documentation (e.g., data dictionaries, file specifications, code books, record layouts, etc.) related to the detailed, as-built design or maintenance of an electronic system containing permanent records, use the GRS item Documentation Necessary for Preservation of Permanent Electronic Records.
DISPOSITION: Temporary. Cut off after system is superseded by a new iteration, or is terminated, defunded, or when no longer needed for administrative, legal, audit, or other operational purposes. Destroy 5 years after cutoff.
AUTHORITY: GRS 3.1, item 011 (DAA-GRS- 2013-0005- 0007)
PRIVACY ACT: Not Applicable
FORMER FILE NUMBER: 1601-01.1
FILE NUMBER: 1601-01.1 – Consolidated into 1601-01, 1606-02 or 1606-11, as applicable.
FILE NUMBER: 1601-01.2 – Consolidated into 1606-02
FILE NUMBER: 1601-01.3 – Consolidated into 1601-02

FILE NUMBER: 1601-02
FILE TITLE: System Access Records - Systems not requiring Special Accountability for Access
FILE DESCRIPTION: User identification and authorization records generated according to preset requirements, typically system generated. A system may, for example, prompt users for new passwords every 90 days for all users. These records are created as part of the user identification and authorization process to gain access to systems. Records are also used to monitor inappropriate systems access by users. Includes records such as: • User profiles • Log-in files • Password files • Audit trail files and extracts • System usage files • Cost-back files used to assess charges for system use. Exclusion 1. Excludes records relating to electronic signatures. Exclusion 2. Does not include monitoring for agency mission activities such as law enforcement.
DISPOSITION: Temporary. Cut off and destroy when business use ceases.
NOTE: See 1601-18 for System Access Records Requiring Special Accountability
AUTHORITY: GRS 3.2, item 030 (DAA-GRS-2013-0006-0003)
PRIVACY ACT: Not Applicable
FORMER FILE NUMBER(s): 1601-01.3, 1606-06.2 Current as of 31 October 2024 OSD Records Disposition Schedules
FILE NUMBER: 1601-02.1 – RESCINDED (per GRS Transmittal 23)
FILE NUMBER: 1601-02.2 – RESCINDED (per GRS Transmittal 23)
FILE NUMBER: 1601-02.3 – RESCINDED (per GRS Transmittal 23)
FILE NUMBER: 1601-02.4 – Consolidated into 103-14
FILE NUMBER: 1601-02.5 – Consolidated into 1606-02
FILE NUMBER: 1601-02.6 – Consolidated into 1606-02
FILE NUMBER: 1601-02.7 – Consolidated into 1606-02

FILE NUMBER: 206-25
FILE TITLE: Government Purchase Card and Travel Credit Card Application and Approval Records
FILE DESCRIPTION: Applications by employees for Government credit cards issued in card-holder's name, whether for official travel expenses or for purchasing goods and services. May include: • Application for credit card • Credit release form • Applicant credit report • Cardholder agreement • Acknowledgement of responsibilities and penalties for misuse • Approving official agreement • Certificate of appointment (warrant) • Card training certificate
DISPOSITION: Temporary. Cut off and destroy upon card holder separation or when card is returned to office and destroyed.
AUTHORITY: GRS 1.1, item 090 (DAA-GRS-2018-0003-0001)
PRIVACY ACT: Not Applicable

FILE NUMBER: 219-01
FILE TITLE: Passport Application Records
FILE DESCRIPTION: Records relating to administering the application or renewal of official passports and visas, including: • Copies of passport and visa applications • Passport and visa requests • Special invitation letters • Visa authorization numbers • Courier receipts • Copies of travel authorizations
DISPOSITION: Temporary. Cut off upon submission. Destroy 3 years after cutoff.
AUTHORITY: GRS 2.2, item 090 (DAA-GRS-2023-0002-0002)
PRIVACY ACT: Not Applicable

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.

10 U.S.C. 134, Under Secretary of Defense for Policy; DoD Directive 5105.65, Defense Security Cooperation Agency (DSCA); DSCA Security Assistance Management Manual, Chapter 10, International Training; DoD Directive 5132.03, DoD Policy and Responsibilities Relating to Security Cooperation; Army Regulation 12-15, SECNAVINST 4950.4B, AFI 16-105, Joint Security Cooperation Education and Training ; Public Law 97-195, Foreign Assistance and Arms Export Act of 1961, as amended; E.O. 9397 (SSN), as amended; and E.O. 10450.

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.

MCNET and MCNET O365 do not collect information directly from the public.