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:

USMA Academy Management System (AMS)

2. DOD COMPONENT NAME:

DRAFT

United States Army

3. PIA APPROVAL DATE:

United States Military Academy (USMA)

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
- [ ] Existing DoD Information System
- [ ] Existing Electronic Collection
- [x] 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.

USMA uses AMS (a system of systems) to evaluate candidates for admissions; to conduct management studies of admissions criteria and procedures; to record performance of students and store data of graduates. Information collected and stored include: (See sec. 2a.); application packets from the public; performance counseling; health/physical status and accomplishments; military status; a peer appraisals. Intercollegiate Athletics (ODIA) uses AMS to track potential and existing athletes' 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)*

To verify/validate candidates' identities and fitness for admission to USMA. To enable data matching (eg, commissioning, background investigations) with Army and DoD Systems. Mission-related tracking of performance. To disambiguate permanent records (eg, transcripts).

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

Applicants can choose to not provide data. Non-accepted applicants may opt in to keep their application on file to try for admission the following year. There is no ability to object once enrolled: there will be permanent records containing PII.

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.

Applicants can choose to not apply or apply with incomplete applications. Academy users (eg. students, staff and faculty or contractors) receive the appropriate Privacy Act advisory statement, but have no further ability to scope consent. Non-admitted applicants may opt in to USMA maintaining their application packet.

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.)*

- [x] Privacy Act Statement
- [ ] Privacy Advisory
- [ ] Not Applicable

Individuals who are seeking admissions to the United States Military Academy choose to provide PII in support of the application and the admissions process. AMS provides an appropriate Privacy Impact Statement to the applicants. Students, staff and faculty see a privacy advisory statement upon every log in to AMS.

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

[X]	Within the DoD Component	Specify.	HQDA, Human Resources Command, SJA
[X]	Other DoD Components	Specify.	USMC, USN, USAF, IC
[X]	Other Federal Agencies	Specify.	Internal Revenue Service (IRS), LE when needed
[X]	State and Local Agencies	Specify.	NY State Commissioner of Education (e.g., Prof Engineer)
[X]	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.	Various across the Academy Directorates.
[X]	Other *(e.g., commercial providers, colleges).*	Specify.	US Congress, colleges and scholarship committees, NCAA

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

- [X] Individuals
- [X] Existing DoD Information Systems
- [ ] Other Federal Information Systems
- [ ] Databases
- [X] Commercial Systems

DRAFT

AMS interfaces with multiple LMS (e.g., Blackboard, Canvas). ODIA uses multiple systems to track potential and existing athletes' information. USMA uses FEDRAMP Moderate as the baseline for cloud-based commercial systems.

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

- [X] E-mail
- [X] Face-to-Face Contact
- [X] Fax
- [X] Information Sharing - System to System
- [X] Other *(If Other, enter the information in the box below)*
- [X] Official Form (*Enter Form Number(s) in the box below*)
- [X] Paper
- [X] Telephone Interview
- [X] Website/E-Form

AMS has multiple portals: Candidate, Congressional, Field Force, Cadet and Staff & Faculty. AMS interfaces with multiple LMS & ODIA. AMS E-Doc Mgt System (EDMS) has multiple primary stores: Records & Discipline, Admissions, Registrar, G1/Personnel and USCC.

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.

[X] Yes [ ] No

If "Yes," enter SORN System Identifier A0351-17b USMA

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. 600-E

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

(3) Retention Instructions.

varies from 0-permanent.

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. 3013 Secretary of the Army; 10 U.S.C. 4331, Establishment: Superintendent: Faculty; 10 U.S.C. 4332 Departments and Professors: Titles: 10 U.S.C. 4334, Command and Supervision; US Army Regulation 150-1 USMA Organization, Administration, and Operation and E.O. 9397 (SSN). In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) (3) Information may be disclosed to Members of Congress to assist them in nominating candidates. Parts of the system may be exempt under 5 U.S.C. 552a(k)5 and (k) 6 . or (k) 7 . as applicable

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: 0702-0060, 0702-0061, 0702-0062

SECTION 2: PII RISK REVIEW

a. What PII will be collected *(a data element alone or in combination that can uniquely identify an individual)? (Check all that apply)*

☐ Biometrics	☒ Birth Date	☒ Child Information
☒ Citizenship	☒ Disability Information	☒ DoD ID Number
☒ Driver's License	☒ Education Information	☒ Emergency Contact
☒ Employment Information	☒ Financial Information	☒ Gender/Gender Identification
☒ Home/Cell Phone	☐ Law Enforcement Information	☒ Legal Status
☒ Mailing/Home Address	☒ Marital Status	☒ Medical Information
☒ Military Records	☒ Mother's Middle/Maiden Name	☒ Name(s)
☒ Official Duty Address	☒ Official Duty Telephone Phone	☒ Other ID Number
☒ Passport Information	☒ Personal E-mail Address	☒ Photo
☒ Place of Birth	☒ Position/Title	☐ Protected Health Information (PHI)[1]
☒ Race/Ethnicity	☒ Rank/Grade	☒ Religious Preference
☒ Records	☒ Security Information	☒ Social Security Number (SSN) *(Full or in any form)*
☒ Work E-mail Address	☒ If Other, enter the information in the box below	

Academic grades, physical fitness grades, military classes/cources (distinct from academic courses) grades, USMA disciplinary records, Honor System records, PHI when converted to PII (as USMA not a covered entity), potential and current athlete data

If the SSN is collected, complete the following questions.

(DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

☒ Yes ☐ No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

LTG Darryl A. Williams, Superintendent, USMA. Dated 23 April 2019.

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

AMS does not depict SSN after entry by the applicant to general users. Academy applicants receive a machine generated temporary identifier. Upon in-processing, the cadet receives a "C Number," an 8 digit identifier. Army G1 requires the SSN as a component of an output report for commissionees/graduates to ensure accurate importation into other Army systems.

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?
If "No," explain.

☒ Yes ☐ No

USMA has created and maintains a C number, a letter "C" followed by 8 numerals as the disambiguator. USMA, on graduation, publishes the 'Cullum Number' of each graduate to the Federal Register.

b. What is the PII confidentiality impact level[2]? ☒ Low ☐ Moderate ☐ High

[1]The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

[2]Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

c. How will the PII be secured?

(1) Physical Controls. *(Check all that apply)*

- [x] Cipher Locks
- [x] Combination Locks
- [x] Key Cards
- [x] Security Guards
- [x] Closed Circuit TV (CCTV)
- [x] Identification Badges
- [ ] Safes
- [ ] If Other, enter the information in the box below

(2) Administrative Controls. *(Check all that apply)*

- [x] Backups Secured Off-site
- [x] Encryption of Backups
- [x] Methods to Ensure Only Authorized Personnel Access to PII
- [x] Periodic Security Audits
- [x] Regular Monitoring of Users' Security Practices
- [ ] If Other, enter the information in the box below

(3) Technical Controls. *(Check all that apply)*

- [ ] Biometrics
- [x] Encryption of Data at Rest
- [x] Firewall
- [x] Role-Based Access Controls
- [x] Virtual Private Network (VPN)
- [ ] Common Access Card (CAC)
- [x] Encryption of Data in Transit
- [x] Intrusion Detection System (IDS)
- [ ] Used Only for Privileged (Elevated Roles)
- [x] If Other, enter the information in the box below
- [ ] DoD Public Key Infrastructure Certificates
- [x] External Certificate Authority Certificates
- [x] Least Privilege Access
- [x] User Identification and Password

Once logged in, Role Based Access Controls in various systems and sub-systems limit the data to which each user has access. USMA also mandates commercial multi-factor authentication for users.

d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?

USMA has purchased and is implementing 'comply to connect' capabilities to improve end-point-protection of systems that access AMS data. USMA has also purchased and is implementing data loss prevention (DLP) capabilities to protect data in the various systems/sub-systems of AMS. USMA has also purchased cloud-based SIEM and logging capabilities to improve traceability of access to AMS data.

SECTION 3: RELATED COMPLIANCE INFORMATION

a. Is this DoD Information System registered in the DoD IT Portfolio Repository (DITPR) or the DoD Secret Internet Protocol Router Network (SIPRNET) Information Technology (IT) Registry or Risk Management Framework (RMF) tool[3]?

[X]	Yes, DITPR	DITPR System Identification Number	2628 (USMA AMS)
[ ]	Yes, SIPRNET	SIPRNET Identification Number	
[X]	Yes, RMF tool	RMF tool Identification Number	2746 - USMA WREN
[ ]	No		

If "No," explain.

b. DoD information systems require assessment and authorization under the DoD Instruction 8510.01, "Risk Management Framework for DoD Information Technology".

Indicate the assessment and authorization status:

[X]	Authorization to Operate (ATO)	Date Granted:	8/1/2020
[ ]	ATO with Conditions	Date Granted:	
[ ]	Denial of Authorization to Operate (DATO)	Date Granted:	
[X]	Interim Authorization to Test (IATT)	Date Granted:	9/30/2019

DRAFT

(1) If an assessment and authorization is pending, indicate the type and projected date of completion.

Dates above are for IATT and projected date for ATO.

(2) If an assessment and authorization is not using RMF, indicate the projected transition date.

c. Does this DoD information system have an IT investment Unique Investment Identifier (UII), required by Office of Management and Budget (OMB) Circular A-11?

[X] Yes [ ] No

If "Yes," Enter UII: WREN: DA30935 If unsure, consult the component IT Budget Point of Contact to obtain the UII

[3]Guidance on Risk Management Framework (RMF) tools (i.g., eMASS, Xacta, and RSA Archer) are found on the Knowledge Service (KS) at https://rmfks.osd.mil.