DRAFT

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:

United States Army

United States Military Academy (USMA)

3. PIA APPROVAL DATE:

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
- ☒ 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
- ☒ 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 coordinate admissions assessments with Congressional Delegations and Admissions' Field Force; to conduct live and non-live data/management studies of admissions criteria and procedures; to record performance of US citizen and international cadets/students across multiple dimensions (e.g., academic, physical, military, character); to integrate with Cadet Treasurer and multiple business processes across the Military Academy Direcorates (MADs); to store, process, and analyze end of course feedback; to store, process, and analyze peer and chain of command performance counseling/assessment; to store indicators of cadet health and medical community recommended mitigations (though not PHI in accordance with guidance from MEDCOM representative); to store information for staff, faculty, and coaches of the Directorate of Intercollegiate Athletics (ODIA) about potential recruits, recruited athletes, and athletes in NCAA and club sports. The types of information USMA collects and stores in AMS include: full social security numbers (SSN), citizenship data, drivers license data, employment information, home/cell phone number, mailing and home address, barracks room assignment, military records, official duty address, passport information, place of birth, race/ethnicity, records, work email address, birth date, disability information, education information, financial information, law enforcement information, marital status, mother's middle/maiden name, official duty telephone number, personal email address, position/title, rank/grade, security information, child information, DoD ID Number, Emergency Contact information, Gender/Gender Identification, Legal Status, Medical Information, Name(s), Other ID Number, Photo, and Religous Preference.

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. To enable data matching with non-DoD systems (e.g., Internal Revenue Service, Department of Homeland Security, Department of State). USMA mission-related tracking of performance of cadets. To disambiguate permanent records (e.g., transcripts), especially for graduates who left the academy before DoD established EDI-PI numbers.

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.

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 to data capture and storage once cadets enroll: there will be permanent records containing PII and other Privacy Act Protected data. Permanent records are necessary as part of USMA's maintenance of its accreditation as an academic institution (e.g., transcripts).

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.

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 on a yearly basis.
------The Candidate Portal displays the following text--------
AGENCY DISCLOSURE NOTICE – The public reporting burden for this collection of information is estimated to average 195 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comment regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense Washington Headquarters Service, Executive Services Directorate, Directives Division, 4800 Mark Center Drive, East Tower, Suite 02G09, Alexandria, VA 22350-3100 (0702-0061). Respondents should be aware that notwithstanding any other provision of the law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR REPSONSE TO THE ABOVE ADDRESS. Responses should be sent to West Point Admissions, 606, Thayer Road, Building 606, West Point, NY 10996

PRIVACY ACT STATEMENT AUTHORITY: Title 5 United Sates Code, Government Organization and Employees, Ch 403, Sec 4346; Ch 505, Sec 5031; Ch 603, Sec 6958; Title 44, United States Code, Public Printing and Documents, Ch 31, Sec 3101; Executive Order 9397, Numbering System for Federal Accounts Relating to Individual Persons. PRINCIPAL PURPOSE: Collection of data on Academy candidates for opening a file. ROUTINE USE: To gather information on a candidate in order to open a file for admissions to the United States Military. DISCLOSURE IS VOLUNTARY. However, failure to provide information could preclude appointment. In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, these records contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows: Academic transcripts may be provided to educational institutions for the purpose of admissions to further educational degree programs. The DoD Blanket Routine Uses set forth at the beginning of the Army's compilation of systems of records notices also apply to this system.
------The AMS Faculty Portal displays the following text--------
By clicking log in below, you acknowledge and consent to the following rules of conduct and policies when accessing the United States Military Academy (USMA) network, to include the Internet:

In Accordance With (IAW) Army Regulation (AR) 25-2 para 4-5m(7), "YOU ARE ACCESSING A U.S. GOVERNMENT(USG) INFORMATION SYSTEM (IS) THAT IS PROVIDED FOR USG-AUTHORIZED USE ONLY. By using this IS (whichincludes any device attached to this IS), you consent to the following conditions: The USG routinely intercepts andmonitors 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 ormonitoring of the content of privileged communications, or work product, related to personal representation orservices by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential." See also United States Corps of Cadets (USCC) Regulations and policies, USMA Regulations and policies, Army Regulation (AR) 25-1, AR25-2, the Joint Ethics Regulation and the USMA Acceptable Use Addendum. In general these references remind users to do nothing that is illegal, immoral, or unethical.

This paragraph applies to USMA's Cadets. Cadets' class-specific laptops, accessories, and tablets bought by cadets are personal equipment that USMA authorizes to connect to USMA's Defense Research and Engineering Network(DREN). The authorization has several conditions:

USMA registers the device; where feasible (e.g., laptop), the device must use a USMA provided IS 'image,'; USMA retains remote administrative rights and prerogatives to such systems while the cadet is enrolled at USMA; formal exceptions to Army policies regarding personal equipment on USG networks.

Upon cadets' graduation or separation from USMA, cadets' laptops, tables, and accessories cease to have any permission to connect to the USMA DREN. Cadets will receive an up-to-date non-government image for their laptop prior to their departure from West Point.

There is no blanket authorization to connect personal equipment (e.g., gaming systems, phones, computers, tablets) to the DREN. USMA provides exceptions to policy and other authorizations when requested through chains of command to the CIO/G6 and approved by the CIO/G6 or Superintendent.

You acknowledge that in the event of a classified information spillage, the system(s) with the classified data are subject to seizure and, as feasible, forensic wiping to remove the classified data and return, as feasible, of the sanitized device(s).

USMA will treat unauthorized devices discovered on the DREN as an active threat and will investigate and remediate. This includes devices within the physical jurisdiction of USMA that are interfering with USMA's network(s) (e.g., WiFi hotspots in barracks, other radio frequency (RF) emitters degrading USMA's use of RF fornetwork operations).

You are responsible for understanding and abiding with what USMA has authorized (and not authorized) for usage/behavior. Violations of this AUP and any addendums, USMA, Army, DoD, or Joint regulations/policies, may result in consequences including: loss of network access, loss of administrative privileges on government managed system(s), loss of access to network provided service(s); civilian or military administrative action; civilian or military criminal action.

The West Point Privacy Policy is an 10 page document hosted at https://help.westpoint.edu/content/West%20Point%20Privacy%20Policy.pdf.

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

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. USMA also posts a USMA specific privacy policy on its home page advising how and why USMA collects, stores, and processes Privacy Act protected data. See also attached Privacy Act Statement, Privacy Advisory, and USMA Privacy Policy.

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.	Army G1, Human Resources Command, Staff Judge Advocate, Army commands/elements that sponsor cadet internships, Army commands/elements that sponsor cadet military development/training opportunities
☒ Other DoD Components	Specify.	All DoD Services (e.g., Service Academy Exchange Program), Intel Community
☒ Other Federal Agencies	Specify.	Internal Revenue Service, Federal Bureau of Investigation, Department of Homeland Security, Department of State, Federal Aviation Administration,
☒ State and Local Agencies	Specify.	NY State Commission of Education (e.g., Professional Engineer certification/registration)
☒ 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.	Varies by academic year, fiscal year, and Military Academy Directorates' contractual needs
☒ Other *(e.g., commercial providers, colleges).*	Specify.	US Congress, US and non-US colleges/universities, US and non-US scholarship committees, National Collegiate Athletic Association (NCAA), Learning Management System (LMS) vendors (e.g., Blackboard, Canvas), Cloud Service Providers (where necessary)

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

AMS interfaces with multiple Learning Mgt Systems (e.g., Blackboard, Canvas). ODIA uses multiple systems to track potential and existing athletes' information. Various elements of USMA use vendor provided point of sale systems with PCI compliant systems. In Accordance with DISA Cloud Computing Security Reference Guide (SRG), USMA's Authorizing Official established FEDRAMP Moderate as the baseline for cloud-based commercial systems containing PII instead of DISA's Impact Level 4 (IL4) as the baseline.

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

[X] Other *(If Other, enter the information in the box below)*

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. USMA uses DD2875, DA31, and numerous other official DoD and DA forms to collect, store, and process PII. Official forms have their own privacy statements and information disposition requirements on the forms or their establishing regulations/policies.

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.

PII collected and stored within AMS has retention requirements that vary from months to 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.

[X] 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