



U.S. Department of Transportation
Privacy Impact Assessment
Maritime Administration
MARAD

USMMA Campus Solutions
UCAS

Responsible Official

VADM Joanna M. Nunan
Email: NUNANJ@USMMA.EDU
Phone Number: [Telephone Number]

Reviewing Official

Karyn Gorman
Chief Privacy
Office of the Chief Information Officer
privacy@dot.gov





Executive Summary

This Privacy Impact Assessment (PIA) is prepared for the new USMMA Campus Solution (UCAS) system, at the United States Merchant Marine Academy (USMMA or Academy), a part of the Maritime Administration (MARAD), U.S. Department of Transportation (DOT).

The UCAS system is a highly integrated application suite comprised of several functional modules, providing an end-to-end solution through students' academic lifecycles while at the Academy. The system maintains records throughout the entire student lifecycle including potential applicants. Using the UCAS system, prospective students can request information and submit applications for admission. Should they choose to enroll, students, generally referred to as "Midshipmen", will then use the UCAS system to request and accept financial aid awards, enroll in courses, participate in the advising process with USMMA mentors, and receive grades. The Academy and students will use the UCAS system to bill and pay Midshipman Fees, respectively, until they graduate. The UCAS system provides student-facing self-service functionality that allows mobile access. This system will be replacing the current USMMA Student Information System, the Comprehensive Academic Management System (CAMS).

MARAD is publishing this PIA in accordance with the E-Government Act of 2002 because the UCAS system receives, uses, and maintains Personally Identifiable Information (PII) from members of the public, specifically names, addresses, congressional districts, citizenship, gender, social security numbers, scholastic background and high school records, extracurricular and athletic participation, college coursework, medical qualification status, physical qualification status, and academic and non-academic information for students and graduates attending USMMA.

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and iii)



examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.¹

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we collect, store, retrieve, use, and share. It is a comprehensive analysis of how the DOT's electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

- Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- Accountability for privacy issues;*
- Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*
- Providing documentation on the flow of personal information and information requirements within DOT systems.*

Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Department activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.

Introduction & System Overview

The UCAS system is a highly integrated application suite comprised of several functional modules, providing an end-to-end solution through students' academic lifecycles while at the Academy. The UCAS system provides student-facing self-service functionality that allows mobile access. The system maintains records throughout the entire student lifecycle including prospects, who may become applicants, who may be accepted and matriculated into students and graduates of the institution. Using the UCAS system, prospective students can request information and submit applications for admission. Should they choose to enroll, students will then use the UCAS system to request and accept financial aid awards, enroll in courses, schedule meetings with advisors, and receive grades. The Academy and students will use the UCAS system to bill and pay Midshipman Fees, respectively, until they graduate.

Faculty and administrative staff perform various business functions to support the students through the student lifecycle. This system will replace the current USMMA Student Information System, CAMS, which no longer provides service sufficient to effectively collect and manage student information.

¹Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo of M-03-22 dated September 26, 2003).



USMMA is implementing the following modules into the UCAS system:

- Admissions – includes biographic and demographic information on prospective students and applicants provided voluntarily directly to USMMA or indirectly as authorized by the individual through testing agencies and paid recruitment services. Records include academic background and high school records, standardized test scores, a biographical essay, and recommendations and evaluations used to determine qualification for an appointment.
- Financial Aid – includes information provided by the individual to the U.S. Department of Education (ED) via the Free Application for Federal Student Aid (FAFSA) for the purpose of evaluating financial need and other eligibility requirements set forth by ED and Federal Student Aid (FSA).
- Student Records – all academic and non-academic records maintained on matriculated Midshipmen including, but not limited to, class year, major, sailing split, course enrollments and grades, grade point average (GPA), academic standing and enrollment status, U.S. Coast Guard training competencies, physical fitness scores, and medical qualification status.
- Academic Advisement – includes records related to academic advising such as aptitude assessments, advising notes, academic alerts and other documentation related to student success and academic standing.
- Student Financials – a student ledger is used to bill Midshipman Fees and record all sources of payment against those charges including self-pay, scholarships, Department of Veterans Affairs (VA) benefits, 529 payments, and Title IV financial aid (Pell Grants and Direct Loans). Bank account information for students and/or parents is maintained in the UCAS system for the purpose of refunding credit balances and reimbursing travel expenses, but financial transactions are conducted primarily in Federal systems and only documented in the UCAS system.

The following external information will be imported into the UCAS system:

- Medical qualifications -- Department of Defense Medical Examination Review Board (DoDMERB) medical qualification status of applicants from Department of Defense Medical Examination Review Board (i.e., qualified, not qualified, waived, etc.).
- Test Score Files – College Board (SAT) or ACT (ACT) scores from prospective students and applicants who requested scores to be sent to USMMA.



- EdConnect Files – Department of Education files transmitted to USMMA through the Student Aid Internet Gateway (SAIG) mailbox, a tool that allows FSA trading partners to securely exchange batch data with FSA applications. EdConnect software is used to retrieve and import files from the SAIG mailbox, and they are imported into the UCAS Financial Aid module through delivered processes. Those files include Student Aid Reports (SAR), Entrance and Exit Counseling reports, electronically signed Master Promissory Notes (MPN), records from the National Student Loan Database System (NSLDS) for FSA program awards and disbursements, aggregate Title IV aid totals, overpayments, and other information pertaining to eligibility for FSA.

The Regimental Conduct Database, which tracks and processes violations of Midshipman conduct, and the Shipboard Training Database, which maintains information and processes required to send Midshipmen to sea for Sea Year sailing periods, are not incorporated into the UCAS system, but will utilize the UCAS system to gather basic biographic/enrollment data, since it is the Academy's primary system of records for this information.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template is based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3², sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations³.

Transparency

Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act require public notice of an organization's information practices and the privacy impact of government programs and activities. Accordingly, DOT is open and transparent about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

² <http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf>

³ http://csrc.nist.gov/publications/drafts/800-53-Appendix-J/IPDraft_800-53-privacy-appendix-J.pdf



DOT and MARAD System of Records Notices (SORNs) provide transparency about privacy practices regarding the collection, use, sharing, safeguarding, maintenance, and disposal of information about individuals covered under the Privacy Act of 1974, as amended.

The collection of PII to be maintained in the UCAS system is subject to multiple Privacy Act SORNs, specifically:

[DOT/MARAD 012 - Applications to United States Merchant Marine Academy, USMMA](#) - 65 FR 19538 - April 11, 2000

[DOT/MARAD 026 - USMMA Midshipmen Deposit Account Records](#) - 65 FR 19544 - April 11, 2000

[DOT/MARAD 027 - USMMA Midshipman Grade Transcripts](#) - 65 FR 19545 - April 11, 2000

[DOT/MARAD 028 - USMMA Midshipman Medical Files](#) - 65 FR 19545 - April 11, 2000

Where applicable the UCAS system will provide on its website the following information to prospective and current students when supplying PII to the Academy.

1. Statutory authority authorizing the solicitation of the information: 46 U.S. Code § 51302 - Nomination and competitive appointment of cadets; 46 U.S. Code § 51303 - Non-competitive appointments.
2. The routine uses which may be made of the information: Information will be used by the United States Merchant Marine Academy as applicant background information to determine eligibility for appointment during the selection process, and to contact the applicant. Information may be shared within the Department of Transportation and Department of Defense in conjunction with functions required for admission to the Academy.
3. Whether or not disclosure of such information is mandatory or voluntary (required by law or optional) and the effects on the individual, if any, of not providing all or any part of the requested information: Disclosure of the information is voluntary; however, failure to provide the requested information may result in a delay or inability to process the application to the Academy.
4. Principal purpose(s) for which information is intended to be used: The information is used to contact prospective students and inform them of recruiting events, the application and appointment process, and application deadlines.



The collected information is subject to the purposes and routine uses published in the applicable SORN listed above.

In addition, upon submitting a formal application, all prospective students must complete the following release:

By signing this form, I authorize every school that I have attended to release all the requested records and recommendations to the United States Merchant Marine Academy (USMMA). I also authorize employees at USMMA to confidentially contact my current and former schools should they have questions about the information submitted on my behalf.

- I waive my right to review all recommendations and supporting documents submitted by me or on my behalf.
- I DO NOT waive my right to review all recommendations and supporting documents submitted by me or on my behalf.

If second response above, I have chosen not to waive my right to review recommendations and supporting documents. I understand that my decision may lead my counselors or teachers to decline to write recommendations on my behalf or may lead USMMA to disregard recommendations submitted on my behalf. I also understand that refusing to turn over information requested by USMMA may affect consideration for admission.

The applicant's response will be shared with each evaluator from whom the applicant is selecting to provide information on the candidate. Here is the text the evaluator/recommender/school official will see:

When providing contact information for counselors, teachers and/or other evaluators, the applicant authorized every school that they have attended to release all the requested records and recommendations to the United States Merchant Marine Academy (USMMA). The applicant also authorizes employees at USMMA to confidentially contact their current and former schools should they have questions about the information submitted.

Applicant's Right to View Recommendations and Supporting Documentation – [Waived or Not Waived, depending on the applicant's response above]

[If not waived] Applicant has chosen **not to waive** his or her right to review recommendations and supporting documents and acknowledged understanding that this decision may lead counselors or teachers to decline to write recommendations on their behalf or USMMA to disregard recommendations submitted.



Individual Participation and Redress

DOT provides a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, and disclosure of their PII. As required by the Privacy Act, individuals should be active participants in the decision-making process regarding the collection and use of their PII and they are provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

As part of MARAD, USMMA ensures that individuals have the right to: obtain confirmation of whether MARAD has records containing PII relating to them; (b) access the record related to them within a reasonable time, at little if any cost, and in a form that is easily understood; (c) obtain an explanation if a request is denied, and challenge such denial; and (d) challenge records relating to them and, if the challenge is successful, have the record amended.

Under the provisions of the Privacy Act, individuals may request searches of the UCAS system to determine if any records in the system pertain to them. This is accomplished by sending a written request directly to:

Maritime Administration
Attn: Privacy Officer
1200 New Jersey Avenue SE
Washington, DC 20590

Individuals may also request access to their records that are maintained in a SORN in the possession and under the control of DOT by complying with DOT Privacy Act regulations, 49 CFR Part 10. Privacy Act requests for access to an individual's record must be in writing and may be mailed, faxed or emailed. DOT regulations require the request include: a description of the records sought, the requestor's full name, current address, and date and place of birth. The request must be signed and either notarized or include a statement that the submitted information is accurate. The statement must be attested to under penalty of perjury. Additional information and guidance regarding DOT's Privacy program is located on the DOT website, www.transportation.gov/privacy.

Purpose Specification

DOT should (i) identify the legal bases that authorize a particular PII collection, activity, or technology that impacts privacy; and (ii) specify the purpose(s) for which it collects, uses, maintains, or disseminates PII.

The Academy is authorized to collect information related to the matters discussed in the "Introduction and System Overview" discussion above by virtue of its enabling legislation in 46 U.S.C. sections 51301, et seq. This information is required to determine potential



student eligibility and to manage a student’s continued eligibility and status throughout their tenure at the Academy, as well as their academic credentials post-graduation.

Admissions information is considered a collection of information subject to the Paperwork Reduction Act (“PRA”) of 1995 (44 U.S.C. section 3506). Notwithstanding any other provisions of law, no person is required to respond to a collection of information subjects to the requirements of the PRA unless that collection displays a currently valid OMB control number. Admissions information falls within OMB control number 2133-0010, which was renewed August 17, 2022, and is valid through August 31, 2025. As part of the renewal process, USMMA sought public comment on the collection of admissions information and received no comments. The implementation of the UCAS system does not alter the requested information and the existing OMB clearance remains valid.

Data Minimization & Retention

DOT should collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected.

The Academy only collects PII that it needs to evaluate application packages and to service financial aid packages, student records, student financial records, and academic advisement records. As noted earlier in this document, while not specifically collected for that purpose, PII collected through the UCAS system may also be used to track and process Midshipman violations and for Sea Year deployment. The Academy does not collect PII in the UCAS system for other purposes. All records, including PII are retained in accordance with current MARAD record retention requirements (Schedule No. NC1-357-81-02), which may be found at https://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-transportation/rg-0357/nc1-357-81-02_sf115.pdf. Student data shall be retained according to the following schedule:

Data Set	Retention	Approval for Collections	Method of disposal
Prospective Student Records	One (1) year after anticipated entry year	NC1-357-81-02/782	Destroy
Applicants Appointed and Enrolled	Combine with Midshipman Personnel Records (p.174)	NC1-357-81-02/783A	See Midshipman Personnel Records



<p>Applicants Not Appointed, or Appointed and Not Enrolled</p>	<p>One (1) year after anticipated entry year (p.174)</p>	<p>NC1-357-81-02/783B</p>	<p>Destroy</p>
<p>Midshipmen Deposit Accounts</p> <p>Financial records are processed through government financial systems, but transactions are documented in student ledgers in the UCAS system for tracking and student accessibility purposes.</p>	<p>Six years, 3 months after termination of account (p.188)</p>	<p>46 App U.S.C. 1295g</p> <p>NC1-357-81-02/824</p>	<p>Destroy</p>
<p>Midshipman Financial Aid Records</p> <p>Records used to determine eligibility for financial aid, and of awards and disbursement of aid</p>	<p>Five (5) years after graduation or separation from the Academy (p.173)</p>	<p>NC1-357-81-02/780</p>	<p>Destroy</p>
<p>Midshipmen Transcripts</p>	<p>60 years after graduation of class (p.200)</p>	<p>46 U.S.C. 51301 et seq.</p> <p>NC1-357-81-02/855</p>	<p>Transferred to Federal Records Center – Five Years</p> <p>Destroyed- Sixty Years</p>
<p>Commitment Contract</p>	<p>Until Graduation</p>	<p>46 U.S.C. 51301 et seq.</p>	<p>transferred to MARAD for MSCS tracking</p>



Midshipman Personnel Records	Five (5) years after graduation.	NC1-357-81-02/863	Transfer to Federal Records Center – Five Years; Dispose of 60 years after graduation of class (p.203)
All other student information	Five (5) years after graduation or when longer needed for current business, whichever occurs first.	46 U.S.C. 51301 et seq. NC1-357-81-02/781	Destroy

Use Limitation

DOT shall limit the scope of its PII use to ensure that the Department does not use PII in any manner that is not specified in notices, incompatible with the specified purposes for which the information was collected, or for any purpose not otherwise permitted by law.

As noted above, USMMA will not collect PII through the UCAS system except to evaluate application packages and to service financial aid packages, student records, student financial records, and academic advisement records. While not specifically collected for that purpose, PII collected through the UCAS system may also be used to track and process Midshipman violations and for Sea Year deployment. All collections of information through the UCAS system are subject to the SORNs listed above. Student records are covered by the Federal Educational Rights and Privacy Act (FERPA), for which students receive annual notice. This regulation dictates what is required for disclosure of these records and is managed by the Office of the Academy Registrar and covered by USMMA policy.

Data Quality and Integrity

In accordance with Section 552a(e)(2) of the Privacy Act of 1974, DOT should ensure that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the Department’s public notice(s).



For the UCAS system, the primary data loaded was confirmed to be properly formatted and valid. Ongoing, all data is validated by format and integrity controls in the software. Changes to key data will be monitored and audited, where appropriate. All users whose data is managed will be able to request data correction and updates through the USMMA Registrar's Office.

Security

DOT shall implement administrative, technical, and physical measures to protect PII collected or maintained by the Department against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with OMB policies and guidance.

MARAD protects PII with reasonable security safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure. These safeguards incorporate standards and practices required for federal information systems under the Federal Information Security Management Act (FISMA) and are detailed in Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems, dated March 2006, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, dated April 2013.

The UCAS system has a risk profile of "Moderate". This is the lowest acceptable level for a system managing PII. Moderate impact means that the loss of confidentiality, integrity, or availability could, for example, result in significant damage to the organization's assets or in substantial financial loss. While the consequences of these types of data compromise can be quite significant, there is no real-world severe damage or loss of life from moderate-level data hacking.

PII collected and maintained in the UCAS system is safeguarded in accordance with applicable rules and policies and is protected by reasonable security safeguards against loss or unauthorized access, destruction, usage modification or disclosure. Specifically:

- All users, especially those with administrative access, will agree to rules of behavior.
- Access to all UCAS system information is controlled using multi-factor authentication (MFA) for access by required users and administrative users.
- Access to the system is on a "least privilege" model, using profiles, roles, and permissions.
- Data is encrypted at rest using approved database encryption and is encrypted in transit using DOT approved algorithms and processes.



- The availability of the data and system is supported by a recovery plan and redundant storage of the data.
- MARAD/USMMA will continue to assess risk for the UCAS system and annually evaluate the systems risk profile and add/adjust controls, as indicated.

Accountability and Auditing

DOT shall implement effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals

MARAD is responsible for identifying, training, and holding personnel accountable for adhering to MARAD privacy and security policies and regulations. MARAD follows the Fair Information Principles as best practices for the protection of information associated with the UCAS system. Federal and contract employees are given clear guidance in their duties as they relate to collecting, using, processing, and securing data. Guidance is provided in the form of mandatory annual Security and privacy awareness training as well as Acceptable Rules of Behavior.

The UCAS system, both code and databases, is scanned continuously using DOT approved continuous monitoring tools. These results are reported to the MARAD Information System Security Manager (ISSM) and other key personnel for identification and remediation. These items will be tracked by the USMMA IT team and the DOT OCIO, where appropriate.

Any incidents involving possible loss of PII will be reported to the DOT Security Operations Center (SOC) within one hour of identification for reporting to the United States Computer Emergency Readiness Team (US-CERT), as appropriate.

The UCAS system is included in annual security and privacy assessments, along with controlled change and configuration reviews. The MARAD Security Officer and MARAD Privacy Officer conducts regular periodic security and privacy compliance reviews of UCAS consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems.

Responsible Official

VADM Joanna M. Nunan
Superintendent
USMMA



Prepared by: Shelly Nuessle, ISSM

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

DOT Privacy Office - Approved - 04 25 2023