NATIONAL DEFENSE UNIVERSITY
SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

MARCH 2020
FORM 2875

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

SECTION I - REQUESTOR INFORMATION *(To be completed by Requestor)* ☒ Initial Request ☐ Modification ☐ Deactivation

1. NAME *(Last, First, Middle Initial)*	2. ORGANIZATION NATIONAL DEFENSE UNIVERSITY
3. COLLEGE/SCHOOL	4. PHONE *(DSN or Commercial)*
5. JOB TITLE AND GRADE/RANK STUDENT/	6. EDIPI Number *or International Travel Order Number (ITO#)*
7. E-MAIL ADDRESS	8. CAC EXPIRATION DATE (MM/DD/YYYY) N/A
9. OFFICIAL MAILING ADDRESS National Defense University 300 5th Avenue, Bldg 64 Fort McNair, Washington DC, 20319	10. CITIZENSHIP ☐ US ☐ FN ☐ OTHER 11. DESIGNATION OF PERSON ☐ MILITARY ☐ CIVILIAN ☐ CONTRACTOR
12. SYSTEM NAME(S) (*Platform or Applications*) NEIS Enterprise (O365/A5), Blackboard, Blackboard Connect and Academic Wireless	13. ACCOUNT TYPE ☐ STAFF ☐ FACULTY ☒ STUDENT ☐ VOL/ INTERN
14. JUSTIFICATION FOR ACCESS Access required to complete coursework.	
15. IA TRAINING OR CYBER AWARENESS CHALLENGE CERTIFICATION REQUIREMENTS ☒ I have completed Annual Cyber Awareness Training. DATE COMPLETED *(YYYY-MM-DD)*	
16. USER SIGNATURE	17. DATE *(YYYY-MM-DD)*

SECTION II – ENDORSEMENT OF ACCESS BY USERS MILITARY OR GOVERNMENT SUPERVISOR
(If the user is a contractor – provide company name, contract number, and date of contract expiration in Block 19.)

18. VERIFICATION OF NEED TO KNOW ☒ I certify that this user requires access as requested.	19. CONTRACTOR ACCESS INFORMATION *(Required for contractors)* 19a. CONTRACT NUMBER 19b. COMPANY NAME 19c. DATE *(YYYY-MM-DD)*	
20. TYPE OF ACCESS REQUIRED ☒ AUTHORIZED ☐ PRIVILEGED		
21. SUPERVISOR'S NAME *(Print Name)*	22. SUPERVISOR'S SIGNATURE	23. DATE *(YYYY-MM-DD)*
24. SUPERVISOR'S ORGANIZATION/DEPT	25. SUPERVISOR'S E-MAIL ADDRESS	26. PHONE NUMBER

SECTION III – SECURITY MANAGER CLEARANCE VALIDATION

27. TYPE OF INVESTIGATION		28. DATE OF INVESTIGATION *(YYYY-MM-DD)*	
29. CLEARANCE LEVEL		30. IT LEVEL DESIGNATION LEVEL I LEVEL II LEVEL III	
31. VERIFIED BY *(Print Name)*	32. PHONE NUMBER	33. SECURITY MANAGER'S SIGNATURE	34. DATE *(YYYY-MM-DD)*

SECTION IV – SYSTEM OWNER AND CYBERSECURITY APPROVAL

35. SYSTEM OWNER OR APPOINTEE SIGNATURE	36. PHONE NUMBER	37. DATE *(YYYY-MM-DD)*
38. CYBERSECURITY SIGNATURE	39. PHONE NUMBER	40. DATE *(YYYY-MM-DD)*

INSTRUCTIONS

SECTION I – REQUESTOR INFORMATION

The following information should be provided by the user when establishing an NDU account.

(1) Name. The last name, first name and middle initial of the user.
(2) Organization. The user's current organization (NATIONAL DEFENSE UNIVERSITY).
(3) Enter the College name and School you will be attending.
(4) Phone. The telephone number of the user.
(5) Add Grade/Rank.
(6) EDIPI (back of CAC) or International Travel Order number (ITO#).
(7) Email Address. The user's email address.
(8) CAC Expiration Date. Expiration date will determine the account expiration date.
(9) Official Mailing Address. The user's official mailing address.
(10) Citizenship. (US, Foreign National or Other).
(11) Designation of Person. (Military, Contractor or Civilian).
(12) System Name(s). The systems for which this access request is being submitted (i.e. NEIS, O365, Blackboard, etc).
(13) Account Type. (Staff, Faculty, Student, Volunteer/Intern).
(14) Justification for Access. A brief statement is required to justify establishment of an account
(15) IA Training or Cyber Awareness Challenge Certification Requirements. User must indicate if he/she has completed the annual training and the date should be within the current fiscal year.
(16) User Signature. User must digitally sign the Acropolis SAAR form with the understanding that they are responsible and accountable for their password and access to the system(s).
(17) Date. The date that the user signs the form. This date should match the date of your digital signature.

SECTION II – ENDORSEMENT OF ACCESS BY USERS MILITARY OR GOVERNMENT SUPERVISOR

The following information should be provided by the user military or government supervisor.

(18) Verification of Need to Know. This should be checked verifying that the user requires access as requested.
(19) Contractor Access Information. If the user is a contractor the user's contract number, company name and expiration date of the contract should be indicated in this block.
(20) Type of Access Required. Place an "X" in the appropriate box. (Authorized – Individual with normal access. Privileged – Those with privilege to amend or change systems configuration, parameters, or settings.)
(21) Supervisor's Name. The supervisor or representative prints his/her name to indicate that the information on the form has been verified and that access is required.
(22) Supervisor's Signature. The user's supervisor should digitally sign in this block. For DISA users the supervisor that is listed in CMIS is the one that should complete this section.
(23) Date. The date that the supervisor signs the form. This date should match the date of your digital signature.
(24) Supervisor's Organization/Department. The supervisor's organization (i.e. RMD, HRD, NWC, etc.).
(25) Supervisor's Email Address. The supervisor's official email address.
(26) Phone Number. The telephone number of the supervisor.

SECTION III – SECURITY MANAGERS CLEARANCE VALIDATION

The following information should be completed by the user's security manager.

(27) Type of Investigation. The user's last type of background investigation (i.e. NACI, SSBI).
(28) Date of Investigation. Date of last investigation.
(29) Clearance Level. The user's current security clearance level.
(30) IT Level Designation. The user's IT designation (Level I, Level II, or Level III).
(31) Verified By. The security manager or representative prints his/her name to indicate that the user's clearance and investigation information has been verified.
(32) Phone Number. The telephone number of the security manager.
(33) Security Manager's Signature. The user's security manager or his/her representative digitally signs in this block indicating that the user's clearance and investigation information has been verified.
(34) Date. The date the form was signed by the security manager or his/her representative.

SECTION IV– SYSTEM OWNER AND CYBERSECURITY VALIDATION

This section (blocks 35 - 40 should be left blank and is for NDU ITD internal processing.