*National Defense University*
*Eisenhower School for National Security*
*& Resource Strategy (NDU-ES)*

# Application Package Checklist
# For Private Sector Fellows

# E-MAIL/FAX THE NOMINATION PACKAGE TO THE NDU REGISTRAR'S OFFICE

Fax Number: (202) 685-4810
Email: **University-Registrar@ndu.edu**

***Each student nomination package must include the following items:***

- NDU/ES Private Sector Fellow Nomination Form
  *(provided in this pdf document)*
- System Authorization Access Request Form
  *(provided in this pdf document)*
- Acceptable Use Policy
  *(provided in this pdf document)*
- NDU Privacy Act Statement
  *(provided in this pdf document)*
- Education Release Form
  *(provided in this pdf document)*

- One official transcript
  *(highest degree earned)*
- One-page student biography or résumé
  *(include education and career history)*
- Memorandum of Agreement
  *(provided as a separate pdf document)*

Revised – July 2019

# *National Defense University*
# *Eisenhower School for National Security & Resource Strategy (NDU-ES)*

# Private Sector Fellow Nomination Form

**DEADLINES: April 15th Fall Semester, September 15th Spring Semester**)

**Instructions**:

- Form with **all** applicable fields completed **must** accompany every nomination package.
- Complete this form with **all** applicable information and send completed package to the University Registrar's Office via email (PDF File), fax or mail using the contact information below.
- Please do not include additional documentation in package. Incomplete or partial submissions will not be processed.

**Name:** _____ _____ _____ _____
(Title) (Last Name) (First Name) (Middle Name or "NMN")

**Job Title**: _____ **Company**: _____

**Program**: *(Check One)*

☐ National Security Strategy Certificate, Fall Semester (5 months)

☐ National Resource Strategy Certificate, Spring Semester (5 months)

☐ Master of Science, National Resource Strategy, Fall and Spring Semesters (10 months)

**Company Mailing Address**: _____

_____

_____
City State ZIP Code

**Work Phone Number**: _____ **Home Phone Number:** _____

**Primary E-mail**: _____

**(Primary email address is the one you will have access to until you arrive NDU.)**

**Highest Degree Earned (Check one):**

☐ **Bachelor Degree** ☐ **Master Degree** ☐ **Doctorate**

**Please include official transcript from the institution where your highest degree was earned (electronic copy for application - raised seal version on arrival).**
(**Note:** A Bachelor's degree from an accredited college or university is the minimum educational credential required to attend NDU-ES.)

**I certify that I have read this application and instructions, and that, to the best of my knowledge, the information proivided is correct and complete. I understand that if it is found to be otherwise, my application is invalid, or in the event that I am enrolled, I will be subject to dismissal from the National Defense University. I have also reviewed the program selected and agree to complete this program if selected.**

_____
***(Nominee Signature)*** ***(Date)***

**Nominated by:** (To be completed by Company Representative):

_____
(Print name) (Title) (Office Phone Number)

_____
(Signature) (Date)

| | | |
|---|---|---|
| **Email**: University-Registrar@ndu.edu | The National Defense University<br>University Registrar's Office<br>300 5th Avenue<br>Washington, DC 20319-5066 | **FAX**: (202) 685-3920 |

Revised – July 2018

# *National Defense University*
# *Eisenhower School for National Security & Resource Strategy (NDU-ES)*

# Private Sector Fellow Security Information

**Access to Fort McNair and NDU networks:** The Department of Defense (DoD) requires the use of a Common Access Card (CAC) for both physical access to facilities and logon access to DoD networks. The minimum requirements to obtain a CAC card at NDU include: 1) Completion of an FBI fingerprint check, and 2) Submission of a National Agency Check with Inquiries (NACI).

**Security Clearances:** Having a DoD security clearance is NOT required for admission to the Eisenhower School. If you desire to take electives or industry studies requiring a clearance you will be provided information on how to have your company submit clearance information. If you do not have a clearance, time does not permit obtaining one for the sole purpose of attending NDU ES.

Prospective students with a DoD/DSS security clearance satisfies the background requirements. For all other students, NDU will initiate a NACI on receipt of fingerprint submissions.

**SYSTEM AUTHORIZATION ACCESS REQUEST FORM 2875 INSTRUCTIONS**

**STEP 1: Complete and sign an NDU SAAR Form 2875** - 4 Page form for Civilian Students (follows this page)

a. Enter required data in boxes 1, 2, 6, 11, 14, 15, 17, and 18. **NOTE: Please provide a personal email address to which you will have continuous access (i.e. Gmail, Hotmail, Yahoo).*
b. Check box 23a.
c. Enter today's date in box 23c. **NOTE: Must be done BEFORE signing*
d. Digitally sign box 23b. **NOTE: Digital signature requires CAC or PIV; if hand-signed, scan the signed 2875.*
e. Save the signed 2875 as a PDF to your computing device, and/or print it.

**STEP 2: Have your organization's Security Office complete Part III of the Form 2875**

a. Forward your signed 2875 to your organization's Security Office OR print out your signed 2875 and hand-carry it to your Security Office.
b. Your Security Office must complete Boxes 36-40f, and a Security Officer must digitally or hand sign the form. All boxes are required. **NOTE: If hand-signed, scan the signed 2875, save it as a PDF, and proceed to Step 3.*

**STEP 3: Download and save your completed, signed 2875**

a. Browse to the final draft of your fully completed, signed PDF 2875 on your computing device.
b. Save your PDF 2875 one last time using this naming convention: **YourLastName_YourFirstName_2875**. **NOTE: The naming convention for your 2875 is critically important to its processing; please follow directions exactly.*

**STEP 4: Email your 2875 to NDU**

a. Open an email to ndu-stuacctreqforms@ndu.edu
b. Attach your PDF 2875 to the email, ensuring it is correctly named, per Step 3b.
c. Click send.
d. **Bring your printed 2875 with you to NDU as back-up verification.**

# 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<br>NATIONAL DEFENSE UNIVERSITY |
| 3. COLLEGE/SCHOOL | 4. PHONE *(DSN or Commercial)* |
| 5. JOB TITLE AND GRADE/RANK<br>STUDENT/ | 6. EDIPI Number *or International Travel Order Number (ITO#)* |
| 7. E-MAIL ADDRESS | 8. CAC EXPIRATION DATE (MM/DD/YYYY)<br>N/A |
| 9. OFFICIAL MAILING ADDRESS<br>National Defense University<br>300 5th Avenue, Bldg 64<br>Fort McNair, Washington DC, 20319 | 10. CITIZENSHIP ☐ US ☐ FN ☐ OTHER<br>11. DESIGNATION OF PERSON ☐ MILITARY ☐ CIVILIAN ☐ CONTRACTOR |
| 12. SYSTEM NAME(S) (*Platform or Applications*)<br>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<br>☒ I certify that this user requires access as requested. | 19. CONTRACTOR ACCESS INFORMATION *(Required for contractors)*<br>19a. CONTRACT NUMBER 19b. COMPANY NAME 19c. DATE *(YYYY-MM-DD)* | |
| 20. TYPE OF ACCESS REQUIRED<br>☒ 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<br>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.

*National Defense University*
*Eisenhower School for National Security & Resource Strategy (NDU-ES)*

# Privacy Act Statement

- **AUTHORITY**: 10 U.S.C. 2165 (National Defense University: Component Institutions), 10 U.S.C. 2163 (Degree Granting Authority for National Defense University). E.O. 9397, as amended (SSN).
- **PURPOSE**: To confirm attendance eligibility, monitor student progress, produce records of grades and achievements, prepare assignment rosters, and to render management and statistical summaries and reports at the National Defense University for active military, Reserve, National Guard, DoD and other Federal and state civilian, international military and civilian fellow, contractor, and private industry students attached to the National Defense University.
- **DISCLOSURE**: Disclosure of requested information is voluntary. However, failure to provide the requested information may result in the denial of entrance and/or access to the NDU. Failure to furnish the requested information may delay or prevent action on your application.

Fellow:

(Name) (Title)

(Signature) (Date)

*National Defense University*
*Eisenhower School for National Security*
*& Resource Strategy (NDU-ES)*

# *National Defense University (NDU)*

## Educational Records Release Authorization

**Name:**

_____

_____

**(Title: Dr., Ms., Mr.) (Last Name) (First Name) (Full Middle Name)**

By signing this statement and enrolling in a course at the National Defense University, I acknowledge and agree that my education records, including copies of my transcripts and student evaluations, may be disclosed to the company named below for inclusion in official personnel records. No further release is authorized without my expressed written consent.

**COMPANY: _____**

**SIGNATURE: _____**

**DATE_____**

***This release will remain in effect until I rescind in writing to NDU.***

**Acceptable Use Policy (AUP)**

MANDATORY NOTICE AND CONSENT FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS

By signing this document, you acknowledge and consent that when you access Department of Defense (DOD) information systems:

> You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government authorized use only.

You consent to the following conditions:

The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

At any time, the U.S. Government may inspect and seize data stored on this information system.

Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests not for your personal benefit or privacy.

Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DOD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections ofa privilege or confidentiality.

Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DOD policy.

**A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to**

**take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.**

These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DOD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.

All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provide a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

NDU STATEMENT OF INFORMATION SYSTEM USE AND ACKNOWLEDGEMENT OF USER RESPONSIBILITIES

I will use NDU Information Systems for official use and authorized purposes only in accordance with DoD 5500.7-R Joint Ethics Regulation. I will not introduce or process data which the Information System has not been specifically authorized to handle. I understand that all information processed on NDU-controlled Information Systems is subject to monitoring. This includes email and web browsing. I may also be held both criminally and financially responsible for any damages that may occur to the network, systems, other electrical and non-electrical equipment, or computing devices, if my actions are determined to be deliberate, willful, or malicious.

I understand the need to protect all passwords at the highest level of data they secure. I will not share my password or account(s) information with coworkers or other personnel not authorized to access the Information System.

I understand that I am responsible for all actions taken under my account(s) either as an authorized or privileged user and will not attempt to “hack” the network, any connected Information Systems, or gain access to data which I am not authorized to access.

I understand my responsibility to appropriately protect and label all output generated under my account (to include printed materials, USB devices, floppy disks, and downloaded hard disk files).

I understand I must have requisite security clearance and documented authorization (approved by my supervisor of my need-to-know before accessing DoD information and Information Systems.

I understand my responsibility to ensure Privacy Act, and other protected personal information (such as personally identifiable information) is protected while it is being processed or accessed. In computer environments outside the NDU physical data processing installations requiring access to NDU Information Systems (such as remote job entry stations, terminal stations, minicomputers, microprocessors, and similar activities), I know I must ensure appropriate protection of personal and sensitive data.

I understand by signing this document I acknowledge and consent that when I access NDU and/or any DoD Information System:

I am accessing a U.S. Government information system (as defined in CNSSI 4009) that is provided for U.S. Government-authorized use only. I understand I must complete designated IA training before receiving system access.

I understand that security protections may be utilized on NDU information systems to protect certain interests that are important to the Government. For example, passwords, access cards, encryption, or biometric access controls provide security for the benefit of the Government. These protections are not provided for my benefit or privacy and maybe modified or eliminated at the Government's discretion.

I understand that I am prohibited from the following:

Introducing classified information into an unclassified system or environment.

Accessing, storing, processing, displaying, distributing, transmitting, or viewing material that is abusive, harassing, defamatory, vulgar, pornographic, profane, racist, promotes hate crimes, or subversive in nature, or objectionable by nature to include; material that encourages criminal activity or violates any applicable local, state, Federal, national, or international law.

Violating the established security, release, and protection policies for information identified as Classified, Proprietary, Controlled Unclassified Information (CUI), For Official Use Only (FOUO), or Privacy Act-protected during the information handling states of storage, process, distribution or transmittal of such information.

Obtaining, installing, copying, pasting, transferring, or using software or other materials obtained in violation of the appropriate vendor's patent, copyright, trade secret, or license agreement. This includes peer-to-peer file sharing software or games.

Installing any unauthorized software (e.g., games, entertainment software) or hardware (e.g., sniffers).

Knowingly writing, coding, compiling, storing, and transmitting. Or transferring malicious software code, to include viruses, logic bombs, worms, and macro viruses.

Engaging in prohibited political activity.

Using the system for personal financial gain such as advertising or solicitation of services or sale of personal property (e.g.• eBay), or stock trading (i.e., issuing buy, hold and/or sell directions to an online broker).

Engaging in fundraising activities, either for profit or non-profit unless the activity is specifically approved by the Command (e.g.• Command social event fundraisers, charitable fund raisers, etc.).

Gambling, wagering, or placing of any bets.

Writing, forwarding, or participating in chain letters.

Posting personal web pages, using my personally-owned information technology (IT such as personal electronic devices (PEDs), personal data assistants (PDAs), laptops, thumb drives etc.), or non-DISA-controlled information technology on DISA-controlled computing assets.

Any other actions prohibited by DoD 5500.7-R or any other DoD issuances.

Personal encryption of electronic communications is strictly prohibited and can result in the immediate termination of access.

I will immediately report any person suspected of engaging in, or any other indication of, computer network intrusion unexplained degradation or interruption of network services, or the actual or possible compromise of data or file access controls to the appropriate Information Assurance (IA) Management or senior IA Technical Level representatives.

I will not install, modify, or remove any hardware or software (i.e. freeware, shareware, security tools. etc.) without written permission and approval from the Information Assurance Manager (IAM) or senior IA Technical Level representative.

I will not remove or destroy system audit, security event, or any other logs without prior approval from the IAM or senior IA Technical Level representative.

I will not introduce any unauthorized code, Trojan horse programs, malicious code, or viruses into NDU information systems or networks.

I will not allow any user access to the network or any other connected system that is not cleared without prior approval or specific guidance of the IA Management.

I will not use any NDU controlled information systems to violate software copyright by making illegal copies of software.

I agree to notify the organization that issued the account when access is no longer required.

In addition to the above statements of acceptable use for NDU Information Systems, the use of NDU's Wireless Gateway also requires:

Users of any personally-owned mobile device shall ensure the device is kept up-to-date with anti-virus definitions and security vulnerability updates.

All NDU Government-issued devices must be online and physically connected to the NDU wired network once per week, for at least 4 hours, to ensure necessary device patches and anti-virus updates get installed.

ALL MUST READ AND SIGN:

I understand that failure to comply with the requirements of this Agreement will be reported and investigated. The results of the investigation may result in one or all of the following actions:

- Immediate revocation of system access and/or user privileges
- Job counseling, admonishment
- Revocation of Security Clearance
- Uniform Code of Military Justice and/or criminal prosecution
- Disciplinary action, reassignment, discharge, or loss of employment

I HAVE READ, UNDERSTAND, AND WILL COMPLY WITH THE REQUIREMENTS SET FORTH IN THIS AGREEMENT.

Name:

Date:

Signature: