# 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:**

National Defense Science and Engineering Graduate (NDSEG) Fellowship Program

**2. DOD COMPONENT NAME:**

Office of Secretary of Defense

**3. PIA APPROVAL DATE:**

09/27/21

Department of the Air Force

## SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

**a. The PII is:** *(Check one. Note: foreign nationals are included in general public.)*

- [x] 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
- [x] 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.**

The DoD NDSEG Fellowship Program, established in 1989 by direction of Congress, sponsored by the Army, Navy and Air Force, serves as a means of increasing the number of United States (U.S.) citizens receiving doctoral degrees in science and engineering (S&E) disciplines of military importance. The DoD, under the direction of the Office of the Under Secretary for Research and Engineering, Basic Research Office, and the military services, promotes education in science and engineering (S&E) disciplines relevant to the Defense mission. One means of promoting S&E education is through awarding fellowships to encourage promising young scientists to pursue doctoral degrees in designated disciplines. The DoD NDSEG awards are under the authority of 10 U.S.C. § 2191, 32 CFR 168a, National Defense Science and Engineering Graduate Fellowships. The request for applications is necessary to screen applicants, evaluate and select students for award fellowships. All NDSEG applications are submitted electronically via contractor, Integrated Technology Solutions – Joint Venture (ITS-JV) website, www.ndseg.org.The NDSEG contractor is responsible for the daily management of NDSEG program for the fellowship classes. The information collected is used for the NDSEG application, NDSEG terms and conditions form and the execution of the NDSEG three year fellowship award. The types of information collected may include but not limited to applicant/awardee name, address, e-mail address (personal/institution), phone number (home/cell), birth date, education information, financial information, race/ethnicity information, gender information, etc.

**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)*

The NDSEG program collects the PII information to administer NDSEG fellows stipends and health insurance, tuition, and travel invoices throughout the three year fellowship.

**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.

If individuals refuse to disclose information, their monthly stipends may not be processed and IRS information would be inaccurate.

**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.

Once PII is collected, the information will be used throughout the three year fellowship tenure to distribute monthly stipends.

**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

Innovative Technology Solutions JV LLC (dba ITS) and Solutions Through Innovative Technologies, Inc (dba STI-TEC) will comply fully with The Privacy Act of 1974, 5 U.S.C. 552a, which provides protection to individuals by ensuring that personal information collected is limited to that which is legally authorized and necessary and is maintained in a manner which precludes unwarranted intrusions upon individual privacy.

**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. | Some PII information will be shared with DoD entities: OSD Basic Research Office Director, DoD NDSEG Program Manager (AFRL/AFOSR/RTC and PK), and Army Research Office and Office of Naval Research NDSEG program managers post fellowship award. |
| ☒ Other DoD Components | Specify. | Some PII information may be shared for internship purposes only of the NDSEG fellow with DoD entities: OSD Basic Research Office Director, DoD NDSEG Program Manager (AFRL/AFOSR/RTC and PK), and Army Research Office and Office of Naval Research NDSEG program managers. |
| ☒ Other Federal Agencies | Specify. | Some PII information may be shared for NDSEG fellow internship purposes to other agencies who offer fellowships. This varies annually. Some past agencies have been NASA (Jet Propulsion Laboratory, Johnson Space Center, & Pathways Program), Sandia National Labs, etc. |
| ☐ State and Local Agencies | Specify. | |
| ☒ 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. | Innovative Through Solutions-Joint Venture (NDSEG 2021/2022) adheres to The Privacy Act of 1974, 5 U.S.C. 552a.<br><br>Systems Plus, Inc., (NDSEG 2019/2020) adheres to |
| ☒ Other *(e.g., commercial providers, colleges)*. | Specify. | Colleges have the PII due to applicants accepted into PhD programs. They have the information prior to the fellowship application. |

**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

Systems Plus, Inc. databases for NDSEG 2019/2020 classes are NDSEG Fellowship Management Tool (www.applyndseg.sysplus.com) and database Microsoft SQL Server. Integrated Technology Solutions - Joint Venture databases for NDSEG 2021/2022 classes are (www.ndseg.org) and database Survey Monkey.

**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

☐ Other *(If Other, enter the information in the box below)*

All information is collected via the website, www.ndseg.org.

**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.

☐ Yes ☒ No

If "Yes," enter SORN System Identifier

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.

Applications are not pulled by name or other personal identifier. Additionally, all PII is removed prior to reviews to ensure unbiased selection.

**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. N1-AFU-89-25;90-03

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

(3) Retention Instructions.

The NDSEG contractor is instructed by DoD to maintain records for ten years before destroying them.

**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.

32 CFR 168a, National Defense Science and Engineering Graduate Fellowships; 10 U.S.C. 2191.
(a) Establishes guidelines for the award of National Defense Science and Engineering Graduate (NDSEG) Fellowships, as required by 10 U.S.C. 2191.
(b) Authorizes, in accordance with 10 U.S.C. 2191 and consistent with DoD 5025.1, the publication of a regulation which will be codified at 32 CFR part 168b.

**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.

0701-0154, DoD National Defense Science and Engineering Graduate (NDSEG) Fellowship Program, 30 Sep 21

## 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 | |

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.

SSN Justification memo submitted to DoD Privacy on 27 SEP 21.

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

The justification for continued authorized uses of NDSEG fellows' SSN is found in DoDI 1000.30, Acceptable Uses, Interactions With Financial Institutions.

(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".

SSNs are only used in the distribution of stipend payments and for IRS tax purposes.

(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

Each respondent is assigned an unique applicant-ID number when they complete electronic application. The applicant-ID number remains through the NDSEG tenure fellowship. However, the SSN information is collected and used by the NDSEG contractor to disseminate monthly stipends.

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

Systems Plus Inc., also ensures all hardware/software environments reside in a secure environmentally controlled facility with restricted access to authorized IT personnel; all IT personnel with access to the NDSEG IT environment complete security/IA awareness training; servers hosting NDSEG app are mounted in racks residing in a secure room with physical lock; access is controlled by the Senior Management team; and program users are instructed and trained to protect their username and password from disclosure.

(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
- [ ] Regular Monitoring of Users' Security Practices
- [x] If Other, enter the information in the box below

Systems Plus Inc., also provides 24x7 network operations/monitoring with centralized network management system with single dashboard display provides continuous visibility of servers, services, software, websites and networks; maintain a multi-layered firewall with Demilitarized Zone (DMZ) and back-up T1 connections and maintain a maintenance plan/schedule to ensure up-to-date patches/updates and test / verify / validate all sites/applications prior to deployment.
STI-TEC maintains a full spectrum information security program based on DFARS 7012 and NIST 800-171. These include completion of a System Security Plan and Policy/Procedure/Plan documentation, as required under forthcoming DoD Cybersecurity Maturity Model Certification (CMMC) Level 3 requirements, for 17 security domains under CMMC. These controls include the full implementation of the required 130 CMMC security that cover all aspects of physical and logical security. For a complete list of these controls see: https://www.acq.osd.mil/cmmc/docs/CMMC_AG_Lvl3_20201208_editable.pdf

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

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

Systems Plus requires user identification and passwords for fellows to access https://applyndseg.sysplus.com/; maintains a multi-layered firewall with Demilitarized Zone (DMZ).
ITS-JV requires 130 Security controls prescribed for CMMC Level 3. See https://www.acq.osd.mil/cmmc/docs/CMMC_AG_Lvl3_20201208_editable.pdf for a complete listing.

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

The NDSEG Contractor is 100% responsible for the safeguarding of PII as directed in the task order. Systems Plus safeguards include: secure role-based access management is provided with continuous monitor hosted systems/services utilizing Symantec, Veritas, Built-In MS Tools and LanGuard; PII only visible to the program administrator users with a need to know (i.e., project leads and accounting for NDSEG security, validation, and financial purposes only) for the purposes as outlined in Section 2 and 10 of Supporting Statement – Part A, Users' self-reported sensitive information is hidden unless the user opts to display it for review of their entry;o PII are traced/controlled from creation/collection, transmission, storage, usage, to disposal; Encryption standards and Secure Socket Layer (SSL) are implemented.