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:

Base-Enclave.NIPR.GatewayCONUS.Scott.Arnold(B-E.N.GC.Scott.Arnold)

2. DOD COMPONENT NAME:

United States Air Force

3. PIA APPROVAL DATE:

09/16/24

AFMC/AFTC/Arnold Engineering Development Complex (AEDC)

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)*

- ☐ From members of the general public
- ☒ From Federal employees
- ☐ from both members of the general public and Federal employees
- ☐ 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.

The B-E.N.GC.Scott.Arnold, also known as the Arnold Unclassified Network (AUNet) system, is the unclassified base-wide Local Area Network (LAN) for supporting the base operations at Arnold AFB. The circuit-enclave is tasked with providing secure and reliable network connectivity for local and global interchange of information and communications in supporting the mission objectives of the Arnold Engineering Development Center. B-E.N.GC.Scott.Arnold provides the network infrastructure supporting the user workstations, administrative servers, and miscellaneous systems. B-E.N.GC.Scott.Arnold services and equipment include routers, switches, application servers, web servers, print servers, desktop workstations, printers, and PDAs. B-E.N.GC.Scott.Arnold is a unclassified enclave that allows for the exchange of unclassified information to complete required mandated DoD related tasks for DoD Cyber Crime Center (DC3). Sections within the organization such as Human Resource (HR), Security Office, Mission Support (MSS), Logistics Office and Trusted Associate (TA) is subject to handling Controlled Unclassified Information (CUI), which is stored within controlled areas of the system database (file shares) or multipurpose applications that reside on B-E.N.GC.Scott.Arnold.

Types of PII Collected: Name(s); Position/Title; Rank/Grade; Employment Information; Security Information; DoD ID Number; Citizenship; Work E-mail Address; Official Duty Address; Official Duty Telephone Phone; Personal E-mail Address; Mailing/Home Address; Home/Cell Phone; Place of Birth; Birth Date; Emergency Contact; Gender/Gender Identification; Race/Ethnicity; Social Security Number.

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)*

PII is collected/stored for mission-related, identification, and administrative use to meet the demands as a DoD organization in support of a wide range of DoD agencies. The PII collected, used, maintained/stored, or disseminated will be relevant and necessary to accomplish a lawful DoD purpose required by statute or Executive Order.

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.

Individuals can object to collection of PII however the application for employment including determination of employment eligibility can not proceed, nor will civilian employment be considered. Once individuals provide data they do not have the option to object to the personal information being stored in the B-E.N.GC.Scott.Arnold since the employee related information is germane to a specific employee assigned to the organization. Other unstructured files came from employees who already gave their consent to use, collection, and storage of their information from initial collection, part of employee in processing.

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.

Consent to the specific use of PII is given when individuals complete required authorized forms. Individuals must provide consent to complete applications for employment. A voluntary application for acceptance is provided to each individual applicant stating that the collection of personal information will be solicited to facilitate eligibility in the application process.

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

A. Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.
or
1. Solicitation of the Social Security Number (SSN) and date of birth is authorized under the provisions of Executive Order 9397, 13478 and the Privacy Act of 1974 section 3(e)(3). Your SSN is a unique identifier and disclosure is necessary in some circumstances to confirm your eligibility for an Air Force Portal account.
and/or
2. If you choose to provide this site with personal information, including entering information into your user profile, please be advised that other Air Force Portal users may be able to view this information depending on the privacy settings in your profile. You may choose to block your entire profile from view or allow other portal users to view your profile. The default setting is to allow other users to see your profile. If your profile is not blocked, other users will be able to view your name, portal ID, email address, DSN phone number, commercial phone number, branch of service, grade, and rank. You can choose to expose elements of your profile to all Portal users, to your network, or to no one. Profile elements for which you control exposure include your nickname, base, organization, AF Specialty Code, education, training & certifications, goals & training planner, network connections, groups and workspaces.
and/or
3. We will only share the information you give us with another government agency if your inquiry relates to that agency, or as otherwise required by law. We do not share information you give us with any private organizations. The Air Force Portal never collects information for commercial marketing. While you must provide an e-mail address for a response other than those generated automatically in response to questions, comments, or feedback that you may submit, we recommend that you NOT include any other personal information, especially Social Security numbers. The Social Security Administration offers additional guidance on sharing your Social Security number.
and/or
4. The site uses session cookies, i.e., tokens that remain active only until you close your browser, for site management. Information is collected for analytical and statistical purposes, and no personal information is collected using this technology. When you close your browser, the cookie is deleted from your computer. This government computer system uses software programs to create summary statistics, which are used for such purposes as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas. You can choose not to accept these cookies and still use the site. The help information in your browser software should provide you with instruction on how to disable session cookies.

ROUNTINE USES: To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.
• To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.
• In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.
• To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. §§ 2904 and 2906.
• To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.
• To appropriate agencies, entities, and persons when (1) the DoD suspects or has confirmed that there has been a breach of the system of records; (2) the DoD has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.
• To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

h. With whom will the PII be shared through data/system exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

☒ Within the DoD Component	Specify.	USAF; AFOSI - Air Force Office of Special Investigation,
☒ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	Army, Navy, Marines Corps, Space Force
☒ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	As required case by case
☐ 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.	NAS, LLC (TOS contractor) Akima Intra-Data, LLC (FSS II contractor) CW Resources (Ability One contractor) Abacus Technology Corp. (BCITS contractor) CQJV, LLC (TMAS contractor) Burns & McDonnell (FARM contractor) Turner Construction Co. (FARM contractor) exp Federal, Inc. (FARM contractor) Healtheon, Inc. (FARM contractor) Perikin (Hypersonic A&AS contractor) Comply with AFI 33-332, Privacy Act Program, when collecting and maintaining information protected by the Privacy Act of 1974, Title 5, U.S.C., Section 552a. Remove or destroy official records only IAW Air Force Records Information Management System, (AFRIMS) located on the internet at: https://www.my.af.mil/gcss-af61a/afrims/afrims/rds/rds_series.cfm.
☒ Other *(e.g., commercial providers, colleges)*.	Specify.	Various universities - (interns)

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

USAF Systems - Record Defense Information Security System (DISS), Defense Enrollment Eligibility Reporting System (DEERS), Trusted Agent Sponsorship System (TASS), Air Force Personnel Accountability and Assessment System (AFPAAS), Job Order Cost Accounting System (JOCAS)

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)*
☐ In-Person Contact
☒ Paper
☐ Fax
☐ Telephone Interview
☐ Information Sharing - System to System
☒ Website/E-Form
☐ Other *(If Other, enter the information in the box below)*

DoD form 2875, SF-86, SF-182, Trusted Agent Sponsorship System (TASS) Form 1 and 2, Form # IN-1144 State of Tennessee Certificate of Successful Completion of Guard Training

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 F033 USSC A Information Technology

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.

N/A

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. DAA-GRS-2013-0005-0006

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

(3) Retention Instructions.

T 17 - 02 R 03.00 - IT/NSS Information Technology/Network Security Systems -- Destroy 5 years after system satisfying the requirement has been decommissioned, after completion and acceptance of the installation or project is disapproved or cancelled, or after test specifications, results, or recorded performance data is no longer needed.

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.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
5 U.S.C. 301, Departmental Regulations; 5 U.S.C. 302, Delegation of Authority; 10 U.S.C. 133, Under Secretary of Defense for Acquisition and Technology; 10 U.S.C. 2224, Defense Information Assurance Program; 18 U.S.C. 1029 and 1030, Fraud and Related Activity in Connection with Access Devices and Computers; 44 U.S.C. 3536, National Security Systems; E.O. 10450 Security Requirements for Government Employees, as amended; Department of Department Instruction (DODI)8500.2, Information Assurance (IA) Implementation, 6 February 2003; Chairman Joint Chiefs of Staff Manual (CJCSM) 6510.01, Defense-In-Depth: Information Assurance (IA) And Computer Network Defense (CND), 25 March 03; Department of Defense Directive (DODD) 8570.1, Information Assurance Training, Certification, and Workforce Management, 15 August 2004; and E.O. 9397 (SSN).

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.

Base-Enclave.NIPR.GC.Scott.Arnold does not collect from members of the public.

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 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 DAF Privacy.

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

Authorized Uses:

a. The justification(s) for the use of the SSN in accordance with DoDI 1000.30, Enclosure 2 are:Paragraph 2.c (2) "Law Enforcement, National Security, and Credentialing," necessary for the Office of Special Investigations Det. 106 at Arnold, Arnold AFB Operations Center, and Security Forces to have this personnel information, which is stored on the system. These offices report and track individuals, and make application information available to other agencies, using the SSN. This includes, but is not limited to, checks of the National Crime Information Center; State criminal histories; and Federal Bureau of Investigation records checks.

b. Paragraph 2.c (3) "Security Clearance Investigation or Verification," as SSNs are necessaryfor security clearance to be hired as an employee of Arnold AFB and receive a Common Access Card (CAC). CAC information is used when logging onto and using the Base-Enclave.NIPR.GC.Scott.Arnold and accessing any applications located on the system. A fileshare overseen by the Personnel Division (DP), is used to manage the DoD Contractor CAC program through the Trusted Agent Sponsorship System (TASS). The requirements for this program are driven by DoD, which requires the use of the TASS Form 1 or 2, in which SSNs are used for credentialing (2.2) and verifying security clearances/vetting (2.3) requirements have been completed prior to CAC issuance. This file share is restricted to those that need to use it to perform functions associated with TASS. Without the use of SSNs, the Personnel Office would not be able to perform their hiring duties.

c. The AEDC Information Protection Office (IP) requires the use of Social SecurityNumbers as indicated in paragraph 2.c (3), as AEDC/IP handles all initiations, verifications, and reporting requirements for AEDC personnel which requires the use of SSNs. Per DoDM 52022.02, AFMAN 16-1405, the IP office is required to maintain files for each subject who has successfully begun an investigation. This requires the subject to complete a SF-86 which requires SSNs, as well as other PII related information. Additionally, SSNs are the primary identification used for security verifications in the Security System of Record Defense Information Security System (DISS). Without the use of SSNs, AEDC/IP could not perform the required duties pertaining to personnel security related functions.

d. Paragraph 2.c (5) "Confirmation of Employment Eligibility," necessary for AEDC/DP(Personnel) to confirm employment eligibility for Federal Civilian Employees (2.5) who come on board. These file shares are accessible only by employees within the personnel office. Arnold

☒ Encryption of Data at Rest	☒ Encryption of Data in Transit	☒ External Certificate Authority Certificates
☒ Firewall	☒ Intrusion Detection System (IDS)	☒ Least Privilege Access
☒ Role-Based Access Controls	☒ Used Only for Privileged (Elevated Roles)	☒ User Identification and Password
☒ Virtual Private Network (VPN)	☐ If Other, enter the information in the box below	

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

Training, continuous monitoring, routine NIPRNet security patches

NOTE: Sections 1 above is to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy. A Component may restrict the publication of Sections 1 if they contain information that would reveal sensitive information or raise security concerns.