



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Anniston Army Depot SharePoint Portal (ANAD SHAREPOINT)

Army Materiel Command (AMC) / TACOM Life Cycle Management Command (LCMC)  
Anniston Army Depot (ANAD)

### SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

- (1) Yes, from members of the general public.
- (2) Yes, from Federal personnel\* and/or Federal contractors.
- (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.
- (4) No

\* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

**SECTION 2: PIA SUMMARY INFORMATION**

a. Why is this PIA being created or updated? Choose one:

- New DoD Information System
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- Yes, DITPR      Enter DITPR System Identification Number
- Yes, SIPRNET      Enter SIPRNET Identification Number
- No

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- Yes
  - No
- If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. 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 should be consistent.

- Yes
  - No
- If "Yes," enter Privacy Act SORN Identifier

DoD Component-assigned designator, not the Federal Register number.  
Consult the Component Privacy Office for additional information or  
access DoD Privacy Act SORNs at: <http://www.defenselink.mil/privacy/notices/>

or

Date of submission for approval to Defense Privacy Office   
Consult the Component Privacy Office for this date.

**e. Does this DoD information system or electronic collection have an 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**

**Enter OMB Control Number**

**Enter Expiration Date**

**No**

**f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.**

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) 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) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect 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) 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 should be identified.

5 U.S.C. 301, Departmental Regulations; Pub. L. 106-229, Electronic Signatures in Global and National Commerce; OASD (C3I) Policy Memorandum, subject: Department of Defense (DoD) Public Key Infrastructure (PKI); and OASD (C3I) Memorandum, subject: Common Access Card (CAC).

**g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.**

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

ANAD SharePoint is Anniston Army Depot (ANAD)'s SharePoint portal and is used by both contractor and government employees. The Portal provides the following essential business capabilities: Content management that ensures information reuse and elimination of redundant or obsolete items; Minimizes organizational boundaries by streamlining business information access; Provides integrity and security for ANAD specific information; Provides search capability which improves productivity and access to information; Puts business critical information in one central location to allow multiple people to make better-informed decisions; Provides a single, integrated platform to manage intranet and applications across the enterprise. The ANAD SHAREPOINT Intranet Portal facilitates the integration of information sharing depot wide. Without this core capability, the Depot would be limited in its ability to conduct day to day operations. It contains knowledge resources and provides a consolidated access source for locally developed systems and enterprise solution systems. It provides access to Depot organization pages. It has approximately 4,000 depot users. It is a child of the ANADNET (DA147100) and housed in the BDLG 363 Server Room also known as the ANDC (DA201555).

This DCI serves as a repository for collaborative information, and it is impossible to predict and enumerate the specific elements of PII that might be collected and processed by SharePoint applications. As such, this PIA details potential information that may be present within the DCI. Data owners are responsible for protecting their data and controlling and limiting access accordingly.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The main privacy risks associated with the use of SharePoint to manage assets containing PII are: misuse of information, data spills, and unauthorized account access.

SharePoint is protected by numerous management, operational, internal, and technical security controls implemented in accordance with information assurance standards published DoDI 8500.2 and AR 25-2. These controls include regular security assessments, physical and environmental security, role-based access control, personnel security, identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g. firewalls, intrusion detection systems, antivirus software), annual training, and audit reports.

**h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.**

**Within the DoD Component.**

Specify.

**Other DoD Components.**

Specify.

**Other Federal Agencies.**

Specify.

**State and Local Agencies.**

Specify.

**Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

Depot Contractors with local network access must abide by all rules and regulations set forth for the DoD Component to safeguard PII.

**Other** (e.g., commercial providers, colleges).

Specify.

**i. Do individuals have the opportunity to object to the collection of their PII?**

**Yes**

**No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

Users can submit a request to have their PII removed from a specific SharePoint site. The provision of information is strictly voluntary; however, if a user declines to submit the information, they may not be provided with the service they are requesting.

(2) If "No," state the reason why individuals cannot object.

**j. 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.

Individuals may either submit or decline to submit the requested information. In general, applications are intended to collect information for specific and clearly defined purposes.



**k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.**

**Privacy Act Statement**

**Privacy Advisory**

**Other**

**None**

Describe each applicable format.

Since PII is utilized by SharePoint, but information is not maintained in a Privacy Act system of records, the utilization of such information triggers the requirement for a privacy advisory.

"The Anniston Army Depot SharePoint Environment is approved for UNCLASSIFIED//FOUO information, including Privacy Act Data; however, additional rules and restrictions are placed on FOUO and Privacy Act Data.

Certain areas of SharePoint, such as sites where files can be uploaded or downloaded, may allow posting of content that can be accessed and viewed by others; these areas may impose additional usage guidelines, rules, and restrictions. Users agree to comply with these additional guidelines, rules, and restrictions, including:

1. Access to SharePoint and the ability to login to the portal does not automatically grant access to all areas of available information.
2. Access to SharePoint requires Common Access Card (CAC) authentication and role-based user permissions based on official need-to-know. Only authorized users required to perform the stated mission will be granted rights to access and post data on respective SharePoint sites.
3. Site Administrators will utilize the Deny-All-Allow-By-Exception access to Personally Identifiable Information (PII) and sites, in other words, no one will gain access to a site unless specifically granted access by the Site Administrator.
4. Use of SharePoint's search functionality may also return items to which users are denied access.
5. SharePoint may create and disseminate information to a specific audience within its membership without incurring any obligation to make such information, including items returned by search, generally available at any future time.
6. The security settings and access authorizations of posted content are the responsibility of the Site Administrator.
7. Each FOUO and Privacy Act Data document or site must be appropriately labeled.
8. PII must not be posted to SharePoint to avoid use of another approved system of records.
9. PII needs to be restricted to users on a need-to-know basis.
10. Users should not publicly store employees' personnel records. Examples of personnel records include compensation, rewards, reviews, or appraisals.
11. Users who violate the Privacy Policy for The Anniston Army Depot SharePoint Environment will be immediately reported to their local IASO and PII Coordinator.
12. DOIM does not claim ownership of any personal content posted to SharePoint; however, by submitting content to SharePoint the user grants DOIM a security interest in such content and therefore understands that it can be deleted, reviewed, edited for content, reversed engineered or otherwise examined at the organization's discretion."