Privacy Impact Assessment
for the

Asset Logistics Management Information System (ALMIS)

DHS/USCG/PIA-025

January 29, 2018

Contact Point
Carl Webster
ALMIS System Owner (ISD-Deputy)
United States Coast Guard
(252) 335-6656

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The United States Coast Guard (USCG) uses the Asset Logistics Management Information System (ALMIS) to facilitate its air and surface operations. ALMIS is an asset logistics system that provides maintenance tracking, parts ordering/inventory, and mission information for aviation and surface assets. This Privacy Impact Assessment (PIA) is being conducted because ALMIS collects personally identifiable information (PII) from USCG personnel and members of other federal agencies.

Overview

The base of operations for ALMIS began with the USCG Air Station Elizabeth City in 1940. The command was responsible for flight and maintenance operations for 10 aircraft and 56 personnel. As the needs of the USCG and the command continued to evolve, the Aircraft Repair and Supply Center (ARSC) was formed. This became the central hub for all depot-level maintenance and logistics for the USCG aviation community. As technology advanced, ARSC began using computers to handle maintenance and logistics for aviation assets and crews. ALMIS was eventually created to compile multiple applications into a larger conglomerate system to handle the needs of the USCG.

ALMIS now handles the maintenance, mission scheduling, and logistics for all USCG aviation assets and many surface (boats) assets. ALMIS enables efficient, flexible, and cost-effective aircraft and surface force operations, logistics, and maintenance support. It supports data entry from the start of a mission, recording the mission execution, tracking crew events, asset aging, asset configuration, asset maintenance requirements, asset part replacements, warehouse activities, and procurement actions.

ALMIS also supports the comprehensive maintenance, operations, and logistical support of Coast Guard aircraft at 28 Coast Guard air stations and the Aviation Logistic Center (ALC), previously the ARSC. In addition to Coast Guard aviation, ALMIS is currently supporting small boat forces and patrol boat forces with anticipation of cutter fleet, electronics, and shore assets over the next several years. There are over 19,000 registered users of ALMIS, which include air crews, surface force crews, maintainers, contractors, and senior decision makers at Coast Guard Headquarters.

Along with military and Government civilian users, ALMIS has some users from the U.S. Forest Service (USFS) who use the system to maintain aircraft that were given to the USFS by the USCG as part of 14 U.S.C. § 141, Cooperation with other agencies, and Pub. L. 113-66, Section 1098, National Defense Authorization Act of 2014.[1] These USFS personnel use standard USCG-

[1] National Defense Authorization Act of 2014, *available at* http://jsc.defense.gov/Portals/99/Documents/FY14NDAA.pdf.

configured workstations and USCG-issued Common Access Cards (CAC) to access ALMIS, just like all USCG personnel. USFS data is entered and stored within ALMIS and does not leave the confines of the system or the USCG network. No data is exported or imported.

Currently, ALMIS uses the Social Security number (SSN) on the backend database to associate with a user's account as this is the only unique identifier for military, civilian, and contractor staff. SSNs are necessary to track which individuals worked on what asset and the SSN is the only means by which ALMIS can currently do that due to the numerous types of personnel (USCG military, Government civilian, contractor, USFS personnel) involved. Military and Government civilian SSNs are routinely collected via an encrypted query from the Coast Guard Business Intelligence (CGBI) data warehouse.[2] Contractor SSNs are routinely (manual data pull) collected out of Electronic Questionnaires for Investigations Processing (e-QIP)[3] or from the user via encrypted email or over the phone from the user. USFS personnel SSNs are collected via an encrypted e-mail. SSNs are manually entered into the system by ALMIS account managers who also create the user accounts and assign permissions within the system. ALMIS uses an individual's PII to create a unique account for him or her within the system. This allows ALMIS to assign permissions and track user activities. All other PII is collected via ALMIS Access Request Forms (ARF) and sent to the helpdesk or entered as a Remedy ticket.

ALMIS uses both PII and sensitive personally identifiable information (SPII); PII in the form of the information collected on the ARFs and SPII in the form of the SSN. The SSN is stored securely on the backend database and is associated to a user's account. While system administrators can view SSNs, users do not see and cannot access other users' SSNs. The PII used from the ARFs includes name, rate, rank, and last 4 of the Employee Identification Number (EMPLID).[4] This information is selected in dropdown menus to allow crew members to add themselves to assets for mission scheduling, maintenance, and tracking purposes (*e.g.*, flight hours). ALMIS undergoes comprehensive and detailed control testing and auditing on an annual basis.

ALMIS is a legacy system managed by the ALC and is scheduled to migrate to the Coast Guard Logistics Information Management System (CG-LIMS) within the next couple of years. CG-LIMS is a technology refresh of ALMIS using a commercial-off-the-shelf enterprise asset management and technical data management tool. Furthermore, it will be the next generation logistics system for USCG that provides a centrally managed, integrated logistics information system. It will combine configuration management, maintenance management, supply chain

[2] *See* DHS/USCG/PIA-018 Coast Guard Business Intelligence (CGBI), *available at* https://www.dhs.gov/privacy.
[3] *See* Privacy Impact Assessment for the eOPF System, *available at* https://www.opm.gov/information-management/privacy-policy/#url=Privacy-Impact-Assessments.
[4] The Employee Identification (EMPLID) number is a random USCG-generated number that is issued to USCG personnel to use in lieu of the SSN as an identifier.

management, and technical information management all in one package. ALMIS will be replaced in order to ensure flexibility with the USCG's changing missions and assets.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

14 U.S.C. § 2; 14 U.S.C. § 93; 14 U.S.C. § 102; 14 U.S.C. § 141; 14 U.S.C. § 632; 14 U.S.C. § 648; 44 U.S.C. § 3101; 44 U.S.C. § 3534; Executive Order (E.O.) 9397, *Numbering System for Federal Accounts Relating to Individual Persons*, as amended by E.O. 13478, *Amendments to Executive Order 9397 Relating to Federal Agency Use of Social Security Numbers*; and the National Defense Authorization Act of 2014 (Pub. L. 113-66).

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The USCG will complete a specific ALMIS SORN to provide coverage for the information collected related to asset maintenance and logistics. This SORN will provide more sufficient coverage than the current DHS/ALL-010 Asset Management Records System of Records.[5] SORN coverage for the information collected to grant access to ALMIS is generally provided by DHS/ALL-004 General Information Technology Access Account Records System of Records.[6]

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. The latest Authority to Operate (ATO) for ALMIS was granted on September 24, 2014. A renewed ATO is currently being granted in concurrence with this PIA.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

No. Currently ALMIS retains all records but is scheduled to migrate to CG-LIMS within the next couple of years. The USCG Records Officer has initiated the CG-LIMS NARA retention schedule; disposition pending.

[5] DHS/ALL-010 Asset Management Records System of Records, 80 FR 58280 (September 28, 2015).
[6] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (November 27, 2012).

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Information contained within ALMIS is not subject to the PRA as the information is not collected from members of the public.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

To ensure safety of assets and crews, it is imperative that all users are correctly identified, have the correct permissions, and are authorized for those permissions by the appropriate authorities. In order to do this, ALMIS collects the following information from the following categories of individuals:

USCG Military:

- Social Security number (SSN);
- Common Access Card number (CAC#);
- Personal Identification Number (PIN) for two-factor authentication;
- Name;
- Rate/rank;
- Employee Identification (EMPLID);
- Sector/group;
- Unit Operating Facilities Address Code (OPFAC);[7]
- Work email address;
- Work phone number; and
- Digital signature.

[7] OPFAC is the operating facility number for a unit/base, similar to a ZIP code for a location.

Government Civilians:

- SSN;
- CAC#;
- PIN;
- Name;
- Civilian grade;
- EMPLID;
- Unit OPFAC;
- Work email address;
- Work phone number; and
- Digital signature.

Federal contractors:

- SSN;
- CAC#;
- PIN;
- Name;
- Unit OPFAC;
- Work email address;
- Work phone number;
- Digital signature;
- Contract number;
- Company name; and
- Period of contract performance.

USFS personnel:

- SSN;
- CAC#;
- PIN;

- Name;
- Civilian grade;
- EMPLID;
- Unit OPFAC;
- Work email address;
- Work phone number; and
- Digital signature.

2.2 What are the sources of the information and how is the information collected for the project?

Military and Government civilian SSNs are collected via CGBI. Federal contractor and USFS personnel SSNs are collected out of e-QIP or from the user via encrypted email or by phone. These methods of collection are used to maximize privacy, security, and accuracy without the need for creating additional documents/files containing SPII. SSNs are manually entered into ALMIS by the ALMIS account managers. All other PII (see Section 2.1) about individuals is obtained from the ALMIS ARFs, which users complete to obtain access to certain parts of the system.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No. ALMIS does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

Due to the extensive process of identity verification within the USCG Office of Security and Management (DCMS-34), data accuracy pertaining to each user's information is highly accurate. This process is part of the e-QIP background investigation process. e-QIP is a web-based automated system that facilitates the processing of standard investigative forms used when conducting background investigations for federal security, suitability, fitness, and credentialing purposes. e-QIP allows users to electronically enter, update, and transmit their personal investigative data over a secure internet connection to a requesting agency. This thorough process is performed on every USCG member who requires access to ALMIS and ensures that an individual's identity/information is accurate. However, ALMIS only collects contractor SSNs via e-QIP. Military and government civilian SSNs are routinely collected via an encrypted query from the CGBI data warehouse.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk of over-collection of information, specifically SSN, within the system.

Mitigation: This risk is not mitigated. Because ALMIS is a legacy system, it is not technically or financially feasible to remove SSN at this time. Despite there being no solution in the interim, USCG will not use the SSN as an identifier with the migration to CG-LIMS.

Privacy Risk: There is a risk of inaccurate data within the system.

Mitigation: SSNs are retrieved from approved and vetted sources whenever possible. When SSN is collected over the phone for a small number of ALMIS users, the information is read back to the individual and confirmed for accuracy purposes prior to inserting into the system. Other PII from ALMIS users is obtained from the ARFs to ensure accurate data for each user. All account managers receive extensive training for creating ALMIS accounts and assigning permissions. Annual audits of all users' accounts within ALMIS are performed by account auditors to ensure accurate data for the user and accurate permissions within the system. In addition, should an error occur, database managers for ALMIS can correct the data on the backend of the system. Users can also submit ARFs to update and correct any inaccurate information.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

ALMIS uses SSNs to create a unique ID to link users to their respective account. This ensures that ALMIS properly tracks maintenance, training, financial transactions, and asset use. The CAC# and Personal Identification Number (PIN) is associated with a user's ALMIS account and is used to provide two-factor authentication. The last 4 numbers of the EMPLID is used as a secondary identification in the system to enable crewmembers to locate themselves in the dropdown menus of the system (*e.g.*, John Doe MK[8]2 8830). Crewmembers may use these dropdown menus to add themselves to missions (*e.g.*, search and rescue, ferry flight) and assets (*e.g.*, helicopter, plane). The email address and phone numbers are used to contact and notify customers of account changes. The remaining information is entered into the system as part of the user's regular identification and account information to ensure proper authorized permissions are established at the proper locations.

[8] MK stands for Machinery Technician. It is an example of a rating designation within the USCG.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No.

3.3 Are there other components with assigned roles and responsibilities within the system?

A small number of USFS personnel have access to the system to maintain their aircraft USCG has given them.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that a system administrator could mishandle the information.

Mitigation: All system administrators and users undergo training via the USCG Learning Management System on the uses of PII. Also, all account managers receive extensive training for creating ALMIS accounts and assigning permissions. The annual mandatory training Federal Cyber Awareness Training (FCAC) and training for all USCG Personnel titled, *DHS Protecting Personal Information and DHS Records Management for Everyone,* instructs all participants on how to identify and handle PII as part of their official duties.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information?

Privacy Act Statements are posted on the ALMIS ARFs. An individual's information is only input into ALMIS once that individual has initiated the registration process through submission of the ARFs. Individuals are also provided notice through the publication of this PIA and the DHS/ALL-004 General Information Technology Access Account Record System SORN. USCG is also in the process of completing a new ALMIS SORN that will provide specific notice of this system's information collection.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

ALMIS users have an opportunity to consent or decline uses of their information when reading the Privacy Act Statement during the registration process. This information is voluntary; however, not providing the information may prevent or delay system access.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that USCG does not provide sufficient notice of collection of this information.

Mitigation: This risk is currently unmitigated. The current DHS/ALL-010 Asset Management Records System of Records SORN does not adequately cover the collection of information related to asset maintenance and logistics. USCG is in the process of completing a new ALMIS SORN to sufficiently cover this collection of information to properly mitigate this risk.

Privacy Risk: There is a privacy risk that individuals may not be aware their information is being used within ALMIS.

Mitigation: ALMIS mitigates this risk through the publication of this PIA as well as through the Privacy Act Statement posted on the ARFs. Additional notice is also provided through the publications of the forthcoming ALMIS SORN and the DHS/ALL-004 General Information Technology Access Account Record System SORN.

Section 5.0 Data Retention by the Project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

Currently ALMIS retains all records but is scheduled to migrate to CG-LIMS within the next couple of years. The USCG Records Officer has initiated the CG-LIMS NARA retention schedule; disposition pending.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information in ALMIS is maintained longer than needed for business purposes.

Mitigation: This risk is not currently mitigated. However, the USCG Records Officer has initiated the CG-LIMS NARA retention schedule; disposition pending.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local governments, and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

The USCG allows select USFS personnel access to ALMIS for maintenance and mission scheduling of their C-130 (airplane used for firefighting) assets. The information is accessed via standard USCG-configured workstations with USCG CACs. USFS personnel can access their aircraft asset information in their respective OPFAC, as well as name, rate, rank of USCG personnel who previously used the aircraft prior to its transfer to USFS.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

External sharing is consistent with 14 U.S.C. § 141, Cooperation with other agencies, and Pub. L. 113-66, Section 1098, National Defense Authorization Act of 2014. USCG is completing a new ALMIS SORN to provide more sufficient coverage for the collection, maintenance, and sharing of information related to asset management, maintenance, and logistics as the current version of the DHS/ALL-010 Asset Management Records System of Records SORN does not provide enough transparency of this information collection and sharing.

6.3 Does the project place limitations on re-dissemination?

Yes. All external sharing agreements are governed by a memorandum of understanding (MOU) that has strict data usage and dissemination clauses protecting any transferred information. External agencies (*i.e.*, USFS) are prohibited from sharing the information provided by the USCG.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

ALMIS users can request disclosures of their information via the ALMIS helpdesk. That information is tracked and recorded in the form of an email detailing the type of information requested. The ALMIS helpdesk can then assist in providing the requestor with the requested information. Audit logs are managed by the helpdesk that captures the disclosure event of each request.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that an ALMIS user may disseminate USCG information externally in an unauthorized manner.

Mitigation: This risk is mitigated. ALMIS users sign Non-Disclosure Agreements (NDA) stating they will not share any ALMIS data with any unauthorized parties. This document outlines authorized access, authorized sharing, and handling of sensitive information. The review process for sharing of data is handled via Coast Guard Intelligence Manual, COMDTINST M3800.6; Coast Guard Freedom of Information (FOIA) and Privacy Act Manual, COMDTINST M5260.3; and Executive Order 13556, Controlled Unclassified Information (CUI).

Additionally, all users take annual IT security and privacy trainings, which outline proper and safe handling of information.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

Individuals seeking access to their data may submit a Freedom of Information Act (FOIA) or Privacy Act request in writing to USCG, Commandant (CG-611), 2703 Martin Luther King Jr. Avenue SE STOP 7710, Attn: Freedom of Information Act (FOIA) Coordinator, Washington, D.C. 20593-7710. Individuals may also submit a request to EFOIA@uscg.mil. Additionally, any user who wishes to know what information ALMIS maintains may request a copy of his or her ALMIS Access Request Forms from the ALMIS helpdesk.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals may seek to correct their information through a Privacy Act request as cited in Section 7.1 above. Additionally, users may complete an ALMIS Access Request Form to correct any incorrect information regarding their records.

7.3 How does the project notify individuals about the procedures for correcting their information?

Individuals are provided notification of the procedures to correct their information through this PIA along with forthcoming ALMIS SORN and the DHS/ALL-004 General Information Technology Access Account Record System SORN.

Additionally, users may also contact the ALMIS helpdesk for guidance to correct inaccurate information.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may not be able to correct or access their records.

Mitigation: This risk is mitigated. ALMIS users can correct their information through a Privacy Act request as cited in Section 7.1 above. Additionally, ALMIS users may correct their information by contacting the 24-hour ALMIS helpdesk or by submitting an updated ALMIS Access Request Form to correct any inaccurate or missing information.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

USCG uses agreements, MOUs, and auditing measures to ensure ALMIS data is used for the specified purpose. All SPII, such as SSN, is stored in restricted tables and folders. Only authorized system administrators have access to these backend areas. USCG also uses access logs to track which system administrator accesses which record and at what time and from what machine. System administrators and Information Security (IS) personnel review daily audit log activity to ensure no illicit or inappropriate accesses have occurred. Annual Office of Inspector General (OIG) audits of logs, PII, and system administrator access are also conducted by third-party auditors to ensure compliance with all federal and DHS laws and guidelines.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

ALMIS users are required to complete the mandated *DHS: Protecting Personal Information and DHS Records Management for Everyone* and *DHS: Protecting Personal Information and USCG Federal Cyber Awareness Training*.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access

ALC uses a Segregation of Duties Matrix, which outlines which type of system administrator is permitted to access PII/SPII data elements. Only system administrators who have a validated business need are able to obtain access to SSNs via the backend of ALMIS. This

ensures system administrators have a validated need to know and are given only the permissions necessary to perform their duties. ALMIS users are unable to see or access other users' SSN. However, users are able to view the name, rate, rank, and the last 4 digits of the EMPLID of other users in the system.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

Current ALMIS information sharing MOUs have been reviewed by the program manager, system owner, counsel, and authorizing official. Any revised MOUs will be sent to the USCG Privacy Officer for review.

Responsible Officials

Carl Webster
ALMIS System Owner (ISD-Deputy)
United States Coast Guard
Department of Homeland Security

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security