

Library Authentication Subscription

Statement of Objectives

Combined Arms Command Library Program

1. Introduction and Background

The U.S. Army Combined Arms Command (CAC) Library Program operates a consortium of 18 academic and special libraries supporting Officer, Warrant Officer, and Non-Commissioned Officer professional military education across the Continental United States. The Library Enterprise Division manages an enterprise Ex Libris Alma/Primo VE environment.

The Government requires a commercial, cloud-hosted authentication and proxy solution to provide seamless and secure remote access to both consortium-wide and library-specific licensed electronic resources.

2. Scope

The Contractor shall furnish a commercial off-the-shelf (COTS), Software-as-a-Service (SaaS) library authentication and electronic resource proxy subscription for one (1) enterprise Program Office instance and eighteen (18) individual library instances.

The solution must natively integrate with the Ex Libris Alma / Primo VE environment and preserve existing user access pathways to the maximum extent possible.

The specific administrative and participating entities covered under this scope are defined below:

Instance Type	Library Name
Program Office	U.S. Army Combined Arms Command Library Program
Participating Libraries	
	Aiso Library
	Army Sustainment University Library
	Bruce. C. Clarke Library
	Center for Military History Library
	CW2 Christopher G. Nason Military Intelligence Library
	Cyber Research Center
	Donovan Research Library
	Ike Skelton Combined Arms Research Library
	Morris Swett Library
	Othon O. Valent Learning Resource Center

	Stimson Medical Library
	T2COM HQ Library
	U.S. Army Aviation Technical Library
	U.S. Army Heritage and Education Center Library
	U.S. Army Institute for Religious Leadership – Military Chaplaincy Resource Center
	U.S. Army Soldier Support Institute Library
	U.S. Army Special Warfare Center and School Library
	U.S. Army War College Library

3. Period of Performance

The contract shall consist of an implementation period from 1 March 2027 thru 14 April 2027 a base period of twelve (12) months beginning 15 April 2027, and six (6) twelve-month option periods, exercisable at the Government's discretion.

3.1 Implementation Period

An Implementation Period of Performance shall commence on 1 March 2027 and end on **14 April 2027**.

This period is established to allow a successor Contractor sufficient time to complete all connection, configuration, implementation, testing, and troubleshooting activities. Official commencement of full operational performance shall occur on **15 April 2027**.

The Implementation Period is intended to overlap the current contract's period of performance ending 14 April 2027. The Government will maintain dual-contract coverage during this overlap solely to ensure zero interruption of electronic resource access for users.

3.2 Base Period

Full operational performance of the required authentication and proxy services from 15 April 2027 through 14 April 2028 (12 months).

3.3 Option Periods

Six (6) successive 12-month option periods:

Option Period 1: 15 April 2028 – 14 April 2029

Option Period 2: 15 April 2029 – 14 April 2030

Option Period 3: 15 April 2030 – 14 April 2031

Option Period 4: 15 April 2031 – 14 April 2032

Option Period 5: 15 April 2032 – 14 April 2033

Option Period 6: 15 April 2033 – 14 April 2034

4. Performance Objectives

The Contractor's solution must achieve the following performance objectives:

4.1 Be a fully hosted, centrally managed SaaS solution requiring no installed software on the Government's premises for either administrators or end users.

4.2 Provide secure Single Sign-On (SSO) capability so authenticated users can access all authorized electronic resources without repeated logins during an active session.

4.3 Use Ex Libris Alma as the primary Identity Provider (IdP). The solution shall authenticate users by validating credentials against Alma user records and support standards-based federation (SAML 2.0 and/or OpenID Connect) without storing or persisting user credentials.

4.4 Support both federated and non-federated electronic resources, including resources that require proxy configurations or IP authentication.

4.5 Support attribute-based authorization by validating and passing, at minimum, the user's primary identifier and library affiliation context. This must enable proper access control for both consortium-wide shared resources and library-specific (locally purchased) resources while releasing only the minimum attributes necessary.

4.6 Provide a CAC Library Program branded login page hosted by the authentication service.

4.7 Support authentication from multiple entry points, including (at minimum) the Primo VE discovery layer, Google Scholar, courseware, and student management systems.

4.8 Provide a centralized web-based administrative interface that enables the Library Enterprise Division to manage all 18 libraries from a single console, including the ability to configure resources, manage permissions, and view usage at both the consortium and individual library level.

4.9 Provide comprehensive usage statistics including, at minimum: total accounts, total authentications, usage by date, usage by resource, accounts banned, authentication failures, and usage broken down by each library.

4.10 Enable future growth by allowing the addition of new libraries and locally licensed resources through configuration changes without unplanned service interruption. Any required service interruption shall occur during an established maintenance window approved by the Government and communicated in advance.

4.11 Operate successfully across both Army Unified Directory Services (AUDS) and commercial internet networks.

4.12 Comply with all applicable DoD, Army, and federal requirements including cybersecurity, Section 508 accessibility, and privacy standards.

5. Implementation Requirements

The Government places extreme importance on maintaining continuous access to electronic resources during any transition. Minimal-downtime cutover is required. All implementation, connection, setup, configuration, testing, and troubleshooting activities shall be completed during the Implementation Period (1 March 2027 through 14 April 2027) for an official performance start date of 15 April 2027.

5.1 Implementation Tasks

The Contractor shall perform all implementation activities necessary to assume full operational responsibility for resource authentication from 1 March 2027 through 14 April 2027. Full operational status shall be complete by 15 April 2027. All tasks below shall be completed no later than 14 April 2027.

- a. Participate in Government-hosted Kick-Off Meeting within three (3) business days of award. The meeting shall include the Contractor's designated implementation managers or representatives, Library Enterprise Division staff, and other Government representatives as required.
- b. Refine, finalize, and execute the implementation plan. Within three (3) business days after the Government-hosted Kick-Off Meeting, the Contractor shall submit an updated implementation plan that incorporates award requirements, Kick-Off Meeting details and outcomes, and Government-furnished information. The plan shall include, at a minimum, the implementation schedule; milestones; roles and responsibilities; communication procedures; cutover activities; and rollback procedures. The Contractor shall perform implementation activities in accordance with the Government-accepted implementation plan.
- c. Configure the enterprise Program Office instance and all 18 library instances, replicating existing user access pathways to the maximum extent possible such as

resource origin points, authentication method, identity provider, required user attributes, anticipated dependencies or constraints, proxy or remote-access behavior, and session behavior.

- d. Complete all required technical integrations which includes but is not limited to SAML 2.0 / OpenID Connect with Alma, Primo VE, Google Scholar, courseware, and student management systems. The Government will facilitate metadata exchange with Ex Libris for Alma/Primo VE. Obtain written Government acceptance of successful integration tests.
- e. Perform User Acceptance Testing (UAT) with designated Library Enterprise Division personnel and users from at least three libraries UAT shall include federated and proxied resources, SSO session behavior, and attribute-based authorization for consortium-wide versus library-specific resources.
- f. Provide a CAC Library Program branded login page that matches current visual identity or approved successor design.
- g. Deliver virtual administrator training to the Library Enterprise Division staff prior to go-live.
- h. Execute a controlled cutover no later than 14 April 2027. In conjunction with the Library Enterprise Division staff, the Contractor shall have a documented rollback plan capable of restoring prior services within two (2) hours if critical defects are discovered.

6. Administrative and Support Requirements

6.1 The Contractor shall provide designated Library Enterprise Division/Government personnel with administrative accounts with the permissions necessary to perform assigned administrative functions. Prior to full operational status, the Contractor shall conduct one virtual, instructor-led administrative demonstration for designated personnel. The demonstration shall include sufficient time for Government questions and answers and shall cover, at a minimum:

- a. Accessing and navigating the administrative interface;
- b. Administrative roles, permissions, and account-management procedures;
- c. User access, authentication, authorization, and library-specific versus consortium-wide access settings;
- d. Basic issue identification, troubleshooting, and procedures for submitting and escalating support requests; and

e. Accessing, generating, exporting, and interpreting available system reports, metrics, and usage statistics.

The Contractor shall provide electronic reference materials for subsequent Government use, including administrator guides, quick-reference materials, and links to current product documentation. The Contractor shall provide or provide access to the training materials no later than the date of the virtual demonstration.

6.2 The Contractor shall provide technical support and help desk services capable of rapidly resolving issues with minimal system downtime.

6.3 The Contractor shall maintain and provide a Cybersecurity Incident Response Plan, upon request.

7. Place of Performance

Technical and Help Desk Services shall be performed at the Contractor's facilities. Government access to the administrative console and reporting shall be provided remotely.