STATEMENT OF OBJECTIVES (SOO)

Freedom of Information Act (FOIA) Enterprise Capability Platform: Case Management and End-to-End Workflow

---

1.0 PURPOSE & SCOPE

The U.S. Army Records Management Directorate (ARMD) requires an enterprise-level, secure, and modern Freedom of Information Act (FOIA) and Privacy Act (PA) Enterprise Capability Platform. This platform must deliver a modern case management and end-to-end workflow solution operating horizontally across both unclassified (NIPRNet / Impact Level 5 / IL5) and classified (SIPRNet / Impact Level 6 / IL6) environments.

The scope of this initiative encompasses the procurement, configuration, onboarding, training, and lifecycle support of a performance-based Software-as-a-Service (SaaS) solution. Government data, records, and metadata may be temporarily stored, processed, and transmitted within DoD IL5/NIPR and DoD IL6/SIPR authorized environments, which are outside the Army-managed Microsoft 365 (M365) tenant, utilizing secure, native integrations with the Army's M365 tenant to retrieve and sync records. This platform will standardize FOIA processing across globally dispersed commands, installations, and echelons, reducing administrative burdens, eliminating backlogs, and ensuring full compliance with federal disclosure laws.

2.0 PROGRAM OBJECTIVES

To modernize FOIA processing, the Army seeks a commercial solution that fulfills the following core program objectives:

1. **Modernize the User Experience:** Transition from legacy, fragmented tracking tools to an intuitive, automated, and streamlined lifecycle workspace.
2. **Ensure Absolute Data Security:** Enforce zero-trust principles, ensuring all Government records, metadata, and case files remain entirely within secure, authorized DoD-managed cloud boundaries (IL5/IL6) and secure Army-controlled tenants.

3. **Enhance Search and Processing Efficiency:** Automate data retrieval across disparate repositories using modern native platform tools and APIs, dramatically reducing the response timeline for complex, multi-agency records requests.
4. **Foster Modular Scalability:** Ensure the underlying platform is built on an open, modular architecture that supports rapid capability updates and seamless integrations.

3.0 TECHNICAL & OPERATIONAL OBJECTIVES

The Contractor's proposed solution must achieve the following performance-based outcomes, mapped across five critical operational areas:

3.1 End-to-End FOIA Case Management & Workflow

The platform must automate and manage the entire FOIA and PA request lifecycle within a unified environment.

- **Intake & Tasking:** Deliver automated request intake capability with the ability to assign, coordinate, and track tasks across different Army commands (including ACOMs, ASCCs, DRUs, and installations).
- **Tracking & Milestones:** Provide real-time automated tracking of statutory deadlines, milestones, and warning alerts to prevent response delays.
- **Collaboration:** Enable secure, concurrent, multi-office review and cross-command coordination features to reduce email dependency.
- **Disposition:** Standardize final administrative closure, archiving, and disposition workflows in compliance with federal records retention schedules.

3.2: Native Microsoft 365 Architecture & Federated Search

To maintain strict data security boundaries, the solution must operate natively within the Army's existing Microsoft 365 (M365) tenant.

- **Native Integration & APIs:** Integrate natively with the Army's Microsoft 365 (M365) tenant using approved APIs (such as Microsoft Search and Graph APIs) to search, index, and retrieve records across SharePoint Online, Teams, OneDrive, and Exchange Online.
- **Secure Hosting Boundaries:** Temporarily store, process, and transmit Government records, data, and metadata within secure, authorized DoD IL5/NIPR (unclassified) and DoD IL6/SIPR (classified) environments outside the

Army-managed M365 tenant, provided that secure API synchronization is maintained to safeguard records.

- **Enterprise Integration:** Utilize secure, automated connectors to synchronize and manage case files without exporting data to unauthorized or unaccredited external environments.
- **Audit Trails:** Maintain complete, unalterable system-generated audit logs of all search actions and user activities, accessible by Army administrators.

3.3 Secure Review, Redaction, and Native AI Capabilities

The platform must provide robust tools to review and redact sensitive information securely.

- **Multi-Format Redaction:** Deliver Department of War (DoW)-compliant redaction tools supporting text, images, audio, video, and structured data formats.
- **Data Protection:** Enforce reliable information security controls to safeguard classified data, Controlled Unclassified Information (CUI), and Personally Identifiable Information (PII) with complete reviewer audit logs.
- **Secure AI Assistance:** Leverage native, secure AI-enabled capabilities (such as automated document triage, duplicate detection, and smart redaction suggestions based on FOIA exemptions) that execute natively within the authorized secure M365 tenant or the platform's accredited DoD IL5/IL6 hosting environments, without exporting data to external, unauthorized commercial AI models and adhering to DoD Responsible AI guidelines.

3.4 Compliance Metrics & Reporting

The platform must deliver real-time dashboards and automated analytics to support leadership decision-making and federal compliance reporting.

- **Real-Time Dashboards:** Provide configurable, real-time dashboards for backlog tracking, processing timeliness, and workload distribution tailored for FOIA officers, reviewers, and leadership.
- **Federal Reporting:** Generate error-free, fully automated Department of Justice (DoJ) Annual FOIA Report metrics on demand.

3.5 Enterprise Scalability & Cross-Domain Security Isolation

The solution must be scaled to meet the needs of the global Army Contracting and Records Management Enterprise.

- **User Scalability:** Support distributed operations with 500 or more concurrent active users globally across CONUS and OCONUS environments.
- **System Isolation:** Maintain strict logical and physical separation between the unclassified (IL5) and classified (IL6) instances, preventing cross-domain data spills while maintaining consistent, parallel workflow behavior on both networks.
- **High Availability & Ingestion:** Process large, complex document sets efficiently, ensuring the platform is capable of digesting, indexing, and rendering at least 10,000 pages within a 24-hour window, with system uptime suitable for global operations.

3.6 Low-Code/No-Code Customization

The platform must empower Government administrators with accessible, secure, low-code/no-code configuration tools to adapt and adjust workflows as mission requirements evolve, without requiring proprietary vendor intervention and adhering to Modular Open Systems Approach (MOSA) principles.

3.7 Operational Onboarding, Training, and Technical Support

The implementation must guarantee rapid time-to-value with minimal disruption to ongoing operations.

- **Rapid Deployment:** Deliver a realistic and accelerated timeline transitioning from contract award to full operational capability. This includes delivering an initial onboarding timeline within five (5) business days of award and providing a designated Onboarding Point of Contact.
- **Train-the-Trainer Program:** Provide an effective training program tailored for FOIA officers, reviewers, and system administrators, supported by comprehensive user documentation. The curriculum must support a scalable "Train-the-Trainer" model to allow command-level instructors to independently onboard end-users, with initial and refresher training available.
- **Technical Support:** Deliver routine technical and customer support during core operational hours (0800 to 1600 Eastern Time, Monday through Friday, excluding Federal holidays and Government-directed facility closings). Provide highly reliable emergency technical support for critical system outages, platform downtime, or security incidents on a 24/7/365 basis.

3.8 Public-Facing Portals & Transparency

Integrate optionally with public FOIA reading rooms, automated posting of releasable records, and public request submission portals with live status tracking.

4.0 SECURITY, CYBERSECURITY, & COMPLIANCE CONSTRAINTS

The proposed solution must conform to all applicable security standards and retain the necessary authorizations:

- **Cybersecurity Compliance:** Adhere strictly to the Risk Management Framework (RMF) and NIST SP 800-53 security controls.
- **Authorization to Operate (ATO):** The platform must maintain active FedRAMP High or DoW Impact Level 5 (IL5) authorization for the unclassified environment, and an active DoW Impact Level 6 (IL6) authorization for the classified environment.
- **National Security & Privacy:** Maintain absolute compliance with AR 25-2 (Army Cybersecurity), AR 25-22 (The Army Privacy and Civil Liberties Program), and AR 25-55 (The Department of the Army Freedom of Information Act Program).
- **Section 508:** Ensure the user interface is fully compliant with Section 508 of the Rehabilitation Act to support accessibility.
- **Data Rights & Ownership:** The Government retains exclusive ownership, unlimited rights, and intellectual property rights to all records, files, data, and metadata processed, stored, or transmitted within the platform (in accordance with federal and defense data rights regulations). Absolutely no contractor or third-party proprietary rights, liens, or claims may attach to Government data. The contractor must guarantee the secure, complete, and uncompromised extraction of all Government data and metadata at any time, upon request, contract completion, or termination, in an open, non-proprietary format at zero additional cost to the Government.

5.0 KEY PERFORMANCE METRICS

The success of the platform will be measured by the achievement of these performance thresholds:

- **System Availability:** Achieve a mandatory 99.9% or greater system uptime across both unclassified (IL5) and classified (IL6) environments (Measured as a monthly average covering both core operating hours and emergency periods).

- **Search Ingestion Capacity:** Process, digest, index, and render up to 10,000 pages of complex documents within a 24-hour window (Evaluated per system outage or maximum load event).
- **Emergency Support Response:** Acknowledge and initiate triage for critical system outages, platform downtime, or security incidents within 1 hour or less of occurrence (Measured per critical event on a 24/7/365 basis).
- **Routine Support Response:** Resolve standard technical tickets and customer inquiries within 4 business hours or less (Measured as a monthly average during standard operating hours).
- **Low-Code Modifications:** Successfully implement and deploy workflow configuration changes with zero system downtime (Measured per configuration deployment).
- **Reporting Accuracy:** Generate error-free, fully automated DOJ Annual FOIA Report metrics on demand (Evaluated during standard reporting intervals).