U.S. Immigration and Customs Enforcement

STATEMENT OF OBJECTIVES (SOO)

U.S. Department of Homeland Security
Immigration and Customs Enforcement
Office of Chief Information Officer

Inmate Recognition and Identification System (IRIS) and Mobile Offender Recognition & Identification System (MORIS) – Bi2 Technologies, LLC

August 2025

1. Purpose:

This requirement is for services to provide ICE with immediate access to over 5.025 million booking records across the United States through the nation's only secure, encrypted, real-time national criminal justice data sharing network. This network is based on advanced iris biometric technology, enabling rapid authentication of subject identities. The implementation of this solution supports Presidential Proclamation 108 "Declaring an Emergency at the Southern Border of the United States" and Executive Orders (EO) 14159, "Protecting the American People Against Invasion," and 14165, "Securing Our Borders," by enhancing ICE's capability to quickly and accurately identify individuals encountered during ICE operations.

2. Background:

Bi2 Technologies has developed and maintains the only national, web-based iris biometric network and database. No other organization, public or private, has developed or implemented a comparable capability. This award will grant ICE immediate access to over 5 million booking records for over 1.5 million unique individuals enrolled by more than 247 agencies. By leveraging advanced iris biometric technology, this solution will enable the positive identification of individuals within seconds, significantly enhancing ICE's operational efficiency and accuracy.

3. Scope:

Bi2's Inmate Recognition and Identification System (IRIS) is the nation's only secure, encrypted, real-time national criminal justice data sharing network, based on Iris Biometric technology. MORIS works in conjunction with Bi2's IRIS. MORIS allows law enforcement to authenticate an individual's identity and immediately have access to any information and data previously entered into the IRIS national database.

4. Performance Objectives:

ICE will utilize Bi2 Technologies' solution and data analytics to access over five million booking records across the United States in multiple jurisdictions. ICE will access the Inmate Identification & Recognition System (IRIS) and the Mobile Offender Recognition & Identification System (MORIS).

5. Deliverables:

The Contractor shall provide annual access license for unlimited enterprise licenses for a 12-month period to the IRIS and MORIS solutions, to include:

- The Contractor shall supply 200 IRIS biometric devices to ICE for deployment at designated locations nationwide within 30 days of the award. Additionally, the

Contractor commits to maintaining the operational capability of these systems throughout the duration of the award.

- The Contractor shall support identification/verification against any images produced from ISO 19794-6 and ISO 29794-6 compliant devices.
- The Contractor shall provide ICE with immediate 24/7/365 electronic access to the IRIS database records on agnostic platforms, including Microsoft, Apple, and Android, for both fixed and mobile devices. This access shall be available for an unlimited number of users and support an unlimited number of queries and/or bulk downloads.
- The Contractor shall ensure complete identity and booking records are provided in response to any authenticated identities.
- The Contractor shall provide ICE immediate 24/7/365 mobile access via Bi2 Technologies Mobile Offender Recognition & Identification System (MORIS) on any platform.
- The Contractor shall provide ICE support to configure recurring real-time alerts based on defined criteria in support of continuing and emerging initiatives.
- The Contractor will provide premium help desk support, annual maintenance plan with patch and emergency fixes, and annual software upgrades including major and minor software version releases.
- The contractor shall ensure that, upon logon, the tool displays a splash screen outlining the agency's permissible uses of the system/data. This screen must require the user's affirmative consent to the rules of behavior before granting access.
- The Contractor shall preserve all available monitoring/packet capture data for at least 180 days.
- The Contractor shall provide a Draft Security Plan as part of their proposal response including a plan to work towards FedRamp certification.
- The Contractor will not use any information provided by the agency (query data) for its own purposes or share the information with other customers, business partners, or any other entity.
- The Contractor will ensure that all images submitted by ICE are immediately deleted after processing the images to determine potential matches.
- The contractor shall not use any data from ICE's queries for commercial purposes. Any algorithms, templates, or query results generated from ICE submissions shall not be used for any other customers of the contractor. The contractor shall only use the queries submitted by ICE to maintain an audit log.
- The Contractor must adhere to the ICE Systems Lifecycle Management process. Deliverables and criteria will be tailored according to the specifics of the procured solutions.
- The Contractor must maintain a test environment and provide access to ICE's Test and Evaluation Team to support continuous interoperability testing.

The mobile application must identify the use and safeguard of Law Enforcement Sensitive (LES) and Personally Identifiable Information (PII) maintaining this data in the appropriate Government hosted location, to include:

- The mobile application must adhere to the specified security standards, including those related to data encryption, authentication, authorization, and access controls.
- The mobile application must integrate with establish Role-Based Access Controls (RBAC), ICE Identity and Access Management (IAM) systems, and enterprise Multi-Factor Authentication (MFA) derived identity.
- The mobile application will undergo security vulnerability scanning and must address security vulnerabilities in the designated timeframe.
- The mobile application must comply with federal laws and regulations, including those related to data security, privacy, accessibility, and transparency. Additionally, it must be approved through ICE's Mobile Application vetting processes.
- The mobile application, and associated data, must comply with federal record retention requirements for all related application data, documentation, and communication.
- The mobile application must be compatible with all mobile devices and operating systems currently fielded and in-use within the ICE enterprise.
- The mobile application must be compliant with ICE Mobile Device Management and Mobile Application Management frameworks.

The contractor shall deliver the license access instructions and license keys to the email address no later than 20 calendar days from date of award.

Program Manager, Erica D. Steele, erica.d.steele@ice.dhs.gov

6. Security Requirements

Federal law requires that all government information systems be protected against unauthorized access or use. The Federal Information Security Management Act (FISMA) is the key cybersecurity statute and requires Federal agencies to implement organization-wide cybersecurity programs. The U.S. Department of Homeland Security (DHS) has instantiated FISMA in several organizational publications. (See Appendix A - **General Cybersecurity Contract Requirements**)

7. Place and Period of Performance

The licenses will be accessible to ICE nationwide, ensuring seamless integration and availability across all ICE locations.

This procurement will be for a base period of 12 months.

8. Invoicing and Payment

Vendors must register on www.IPP.gov in order to submit invoices and receive payments. Invoice will not be accepted by any other method.

9. Point of Contacts

Name	Role	Email
Michelle L. Taylor	Contracting Officer	michelle.l.taylor@ice.dhs.gov
Kelli Brooks	Contract Specialist	kelli.brooks@associates.ice.dhs.gov
Lakisha W. Mack	Contracting Officer Representative	lakisha.w.mack@ice.dhs.gov
Jimmy Hackett	Alternate Contracting Officer Representative	jimmy.hackett@ice.dhs.gov
Erica D. Steele	Program Manager	erica.d.steele@ice.dhs.gov