ICE/HSI has a wide range of requirements for a telecommunications analysis system. These requirements include:

SYSTEM ARCHITECTURE, SCALABILITY, AND PERFORMANCE

User Capacity:

- Platform capable of supporting thousands of users.
- Ability to handle at least 500 concurrent users geographically dispersed throughout the U.S. and foreign offices without system degradation or noticeable latency.
- User-friendly functionality.

Data Capacity:

- Unlimited data storage.
- Ability to seamlessly process, search, store, and analyze massive datasets (at least 10 TB, encompassing billions of communication records) with ease.

Web-Based Interface:

- Must include a web-based option that enables users to quickly access data, conduct queries, perform deconfliction, and generate reports without having to log into a full desktop application.

Legacy Data:

- Ability to seamlessly lift, shift, normalize, ingest, and verify the data integrity of all legacy database files and active case data.

Cloud and Infrastructure:

- Must provide Cloud System and Infrastructure Engineering support.
- Centralized database accessible by authorized user, including the ability of users throughout United States and foreign offices to access and analyze data.
- Simplified database management and maintenance.

Methodology:

- Must comply with the AGILE methodology for development and updates.

DATA INGESTION AND LIVE INTERCEPT (CALEA / TITLE III)

Live Intercepts:

- Collection and interception for GPS locations and live call surveillance.

- Integrated live collection and analysis tools in one program for Title III/wiretaps, pen register/trap and trace (telephonic, email, social media, IP address, WhatsApp), and live ping/GPS locations.

CALEA Compliance:

- Ability to receive legacy and current CALEA formats, and maintain compatibility with future CALEA formats.

Data Ingestion:

- Ingestion and normalization of live and historical telecommunications records from diverse sources, including:
    - Phone subscriber information
    - Call detail records (CDRs) or tolls
    - Cell tower location data (including range to tower, timing advance, and tower dumps)
    - GPS locations
    - Cyber tips
    - Web browsing history
    - Email
    - Financial information and transactions
    - Social media records (e.g., Yahoo, Google, Microsoft, Snapchat, Instagram, Facebook, X/Twitter, WhatsApp, others)

Mobile Forensics:

- Ingestion and normalization of cell phone and other mobile device forensic extractions (e.g., from Axiom, Cellebrite, Oxygen, Susteen, XRY).

ANALYTICAL CAPABILITIES, VISUALIZATION, AND MAPPING

Analysis, Search, and Filter:

- Analysis of live and historical telecommunications, email, social media, IP address, financial, and location information.
- Advanced filters, keyword searching, and sort functions.
- Batch query capabilities for communication selectors.

Visualizations:

- Dashboards, reports, graphs, charts, timelines, and other visualizations for the analysis and presentation of data.

Mapping Tools:

- Geo-temporal visual analysis and mapping software used for CDRs, mobile forensic extractions/data, GPS locations, location-tracking data, and social media that runs concurrently with the main system.
- Mapping tools for GPS locations, IP addresses, and other locations of interest.
- Must include a 3D mapping tool running concurrently with the main system.
- Ability to identify Internet Service Providers (ISPs) and map IP addresses.

Alerts:

- Live collection alerts for calls and location-based geo-fence alerts for GPS locations.

Mobile App:

- Must include an integrated mobile/phone application to display live data from the main system.

Exports:

- Export capabilities to external charting, mapping, case management, and database applications.
- Exportable PowerPoints and videos for presentations.

DECONFLICTION AND DATA SHARING

Case Overlap and Deconfliction:

- Advanced deconfliction features that allow users to set a priority for communication IDs/selectors being queried (e.g., target, known contact, unknown contact; high, medium, low priority) and enter comments.
- The system must generate automatic email, text, in-system, and push notification alerts when an overlap/deconfliction occurs.

Interoperability:

- Web-based and integrated interfaces for data sharing and deconfliction with state, local, and federal partner agencies for joint investigations.
- Ability to API with outside vendors to allow queries of data (e.g., public records, internal law enforcement systems, etc.)

Integration:

- Integration capabilities for direct uploads into case management systems, deconfliction systems, and law enforcement subpoena systems.

GENERATIVE AI AND COGNITIVE SERVICES

Integrated AI Assistant:

- An embedded Generative AI assistant (leveraging ICE/HSI-provided Azure AI accounts) enabling users to search, query, filter, interact with, summarize, map, and visualize (e.g., lists, maps, timelines, tables, graphs, charts) complex datasets via natural language prompts to streamline investigative workflows.
- Must enable natural language queries of system help guides, training materials, and quick reference guides to assist users in performing basic navigation and executing all functions within the system.

Cognitive Services:

- Ability to add image tagging, translation and transcription cognitive services interface capabilities (leveraging ICE/HSI-provided Azure accounts).

Security and Compliance:

- The AI assistant must securely reside within the ICE/HSI security boundary.
- Strict compliance with the ICE AI Contract Language, ensuring no ICE/HSI data, user prompts, or derivative outputs are used to train external, public, or commercially available AI models.
- The AI must include comprehensive logging, be fully auditable and traceable, and prevent vendor lock-in. These logs must be securely stored for audit purposes and made readily available to ICE/HSI upon request.

SECURITY, AUDITING, AND ADMINISTRATION

Security Boundary:

- Secure deployment within the ICE/HSI security boundary.

Data Protection and Access:

- Role-based access controls.
- Secure backup storage for evidence.
- Ability to hide/mask sensitive investigative information.
- Ability to designate specific users or groups allowed to view sensitive data.

Audit Logging:

- Comprehensive logging of all AI inputs/outputs.
- Auditing function for system administrators to generate reports on intercepts, data volume and type, users, and system activity that is fully compatible with ICE/HSI's current Microsoft Dynamics 365 contract.

Support and Training:

- Dedicated user support and help desk resources.
- On-site and virtual training programs.

Custom Development:

- Ability to rapidly develop new functionality and features to meet evolving ICE/HSI mission requirements, exploit new technologies, and adapt to emerging criminal trends.