Department of Homeland Security (DHS)
U.S. Customs and Border Protection
(Digital Forensics (DF) Analytics)
REQUEST FOR INFORMATION (RFI)
Release Date: June 20, 2025
Response Date: July 10, 2025

Purpose:

CBP is conducting market research to gain a greater understanding of the full range of available options for Data Analytics systems designed for processing forensically acquired electronic data, including but not limited to text, contacts, video and image data for investigative purposes. This is an RFI released pursuant to Federal Acquisition Regulation (FAR) Part 10 – Market Research and Part 15.201(e). This RFI's purpose is to obtain market information on viable sources of supply, industry practices, answers to specific questions, and industry comments to help inform requirements and future Statements of Work.

Background:

U.S. Customs and Border Protection (CBP), a component of the Department of Homeland Security (DHS), currently uses a wide variety of digital data extraction tools. CBP is interested in obtaining responses to this RFI from prospective offerors that could provide the services and software required to support performing data analytics on extracted data. The Government encourages the responders to this RFI and prospective offerors to propose the most innovative, cost-effective method in achieving the desired objectives and results.

The Government ideally seeks responders to this RFI and prospective offerors that can provide low risk system solutions that are already in production and operational that would only require configuration changes without changes to software code, but at most would require minimal software code changes to satisfy the Government's key requirements. The Government's position is that there is insufficient time for extensive system development while maintaining low risk, therefore, prospective offerors that propose such systems/solutions will likely not be competitively viable.

Scope:

As CBP's nationwide Digital Forensics efforts are expected to expand and be modernized, it is anticipated that CBP efficiency of operations will also increase and be augmented. In fiscal year 2024, CBP processed over 420 million travelers and performed advanced searches on over 4,000 electronic devices. Digital Forensics workload varies across field offices

Objective:

CBP is seeking industry feedback regarding a methodology to accomplish implementation of digital forensics analytics.

Opportunity:

CBP wishes to enhance data analytics to identify patterns and artifacts of interest to support enforcement actions in the field by identifying patterns and artifacts of interest.

CBP envisions this solution to meet at a minimum the following requirements:

For Data Analytics

- Focus on ingestion and analysis of data collected from disparate sources and from a variety of electronic media.
- Able to ingest multiple file types to include standard audio, video, image, text and other file types.
- Able to identify patterns, connections, and leads in support of investigation and other law enforcement action, specifically border enforcement, activities.
- Able to configure user defined access controls.

For context, sample use cases or scenarios include the ability to:

- Integrate data analytics at an enterprise level to help expedite the analysis of data extracted and improve decision making on the ground to further enforcement actions.
  Example: search a list of text messages to find patterns or "hidden language" in suspect communications that may not be obvious at first look.
- Perform data analytics on forensically acquired electronic data including text, images and video.
  Example: a "red tricycle" appears in different videos acquired from different data sets.
- Provide situational awareness on devices and applications that can pose a challenge by preventing access to the data on mobile devices encountered at and in between the ports of entry.
  Example: a new encrypted chat message system that will require new tools and techniques to access.
- Perform data analytics including Artificial Intelligence (AI) to help digest the large amounts of data.
  Example: Be able to analyze a large dataset of text messages from many different uses to find patterns for intel generation.

Schedule:

CBP anticipates calling for sources in FY 26 QTR 2 with qualified sources being provided with a Statement of Work in FY26 QTR 2 and a contract award in FY 26 QTR 3. This schedule is notional and is subject to change.

Responses Requested:

To assist CBP in developing and further refining our requirements, please provide responses to the following questions and requirements. CBP understands that some responses may be conceptual, while others are limited to the type(s) of technologies being considered. Responses should include the following information: See Appendix A

Instructions and Response Guidelines:

RFI responses are due by 3:00 pm on Thursday, July 10, 2025, and shall be limited to a total of 50 pages not including foldouts and full-size page charts. Page size is limited to 8.5 x 11 inches, 12-point font, with 1-inch margins in Microsoft Word format. Both sides of the paper may be used but each side shall be included in the page count unless intentionally left blank.

Please provide the information you deem relevant to respond to the specific inquiries of the RFI. To support budget and planning purposes you may also include rough cost estimates based upon the objectives outlined in the RFI. Information provided will be used solely by CBP as market research and will not be released outside of the CBP Digital Forensics requirements team. This RFI does not constitute a Request for Proposal (RFP), Invitation for Bid, or Request for Quotation, and it is not to be construed as a commitment by the Government to enter into a contract, nor will the Government pay for the information submitted in response to this request. All information contained in this RFI is preliminary as well as subject to modification and is in no way binding on the Government. Responses shall be submitted electronically via email to the Contacting Officer no later than 3:00 p.m. on Thursday, July 10, 2025. The subject line shall read: 70B06C25RFI00137 CBP Forensics Data Analytics. NO SOLICITATION EXISTS AT THIS TIME.

Contact Information:

Contracting Officer: Shaun Saad
Phone number: 202.425-1732
Email address: shaungalen.saad@cbp.dhs.gov

The Government is not required to respond to any information provided in response to this RFI. It is the responsibility of the interested parties to monitor Fedbizopps.gov for additional information pertaining to this RFI.

Appendix A: Interested Vendor Overview Questions

Interested Vendors are requested to submit brief answers to the following:

- **Company Name and UEI Number**

- **Business Size –** *Is your company a small or large business based on 518210 NAICS 518210 Computing Infrastructure Providers, Data Processing, Web Hosting, and Related Services and/or* ***513210****: Software Publishers?*

- **Product/Solution Description**

- Contract Vehicles – *Is your product/solution available on a GWAC? Please provide the identifiers of any such contract vehicles on which your product/solution is available .*

- **System Use –** *Provide a brief description of the number of organizational customers that have acquired the precise product/solution you propose to use/configure/modify to meet CBP requirements, the daily transaction volumes for each organizational customer and the number of users at each organization (if known), along with the specific "mission" or application for which your product/solution is used by each organizational customer and the date when your product/solution began production operations with each organizational customer. For those customers which required configuration please provide the scope of the configuration changes for each customer and how long it took to implement those configuration changes to the customers' satisfaction, prior to system testing. Also include an explanation of whether the product/solution is considered to be a Digital Forensics solution.*

- **Law Enforcement Applications –** *Is your system implemented and in-use in a law enforcement production environment for investigative purposes? If yes, identify each and all organizational customers/system name and references including contact information (i.e. LAPD, FBI, CBP, ICE) as well as when the system reached full operational status with each law enforcement user.*

- **Costs –** *Based on experience and on the descriptions below, provide estimated base and O&M costs using a chart similar to below:*

    - Software licenses – Identify costs associated with the product and any 3rd party software, including annual maintenance
    - Releases/patches – Identify software costs associated with following the recommended upgrade path
    - Labor – Identify labor costs to support the system and cost to install/implement upgrades (based on recommended upgrade path)
    - Hardware Costs – The hardware environment will be provided by the government using the DHS Infrastructure as a Service schedule. Identify any additional hardware costs that may be incurred.
    - Other costs – Identify any other costs associated with supporting the system.

Costs/Period	Base	Year 1	Year 2	Year 3
Software Licenses 3rd Party Software 3rd Party Software				
Releases/Patches				
Labor				
Hardware Costs				
[Other Costs]				
[Other Costs]				

- **Hardware Environment –** *Describe the hardware environment required for production operations and to support your system/solution.*
- **Hardware Environment Transition –** *Describe the capability of the proposed hardware environment required for production operations and to be implemented in a hardened hosted cloud-based service.*
- **Implementation Model –** *How is your solution implemented? For example, is your company the sole implementer or are other companies also able to implement your product? Provide a brief explanation. Examples may include ability to train/certify government experts to maintain; evidence of third-party companies being able to support; etc.*

- **Customizations –** *Explain how software development of customizations (i.e., modifications) would be conducted and managed, if required. For those customization(s) listed earlier which required such customizations, please provide a general description of the scope of those changes and how long it took to develop those changes to the customer's satisfaction, prior to system testing.*

- **Interfaces –** *Describe your system's approach to interfaces, specifically any existing interfaces to law enforcement/other significant entities currently in production and the ability to add new interfaces.*

- **Pre-Implementation Upgrade Path –** *When development of any required customizations is complete, will the most current version of the product be installed? What is your approach for installing patches during development of these customizations?*

- **Post-Implementation Upgrade Path –** *Describe your approach to "routine" product upgrades post-implementation that apply to all of your customers of the proposed product/solution, including how upgrades are handled when customer selects not to upgrade on a scheduled basis. Also, describe your approach of notifying customers of software patches.*

    - *What is the product support posture/cost if the government falls 1, 2, or even 3 major upgrades behind the commercially available solution?*

    - *What level of abstraction or layering will be available such that a major upgrade/core product will have limited impact to configuration changes/customizations based on customer/client need?*

- **Licensing Model –** *Describe your licensing model (i.e. annual, name seats, or perpetual).*

- **Property Rights –** *What are the property rights of your product, including ownership of the source code, in the event of company bankruptcy, sale of company, relationship with customer ends, etc.?*

- **Proprietary Solution –** *Is any part of your system or solution you would propose proprietary? If so, please describe.*