Ministry of Defence

Government of India

REQUEST FOR INFORMATION

BY

MINISTRY OF DEFENCE

GOVERNMENT OF INDIA

FOR PROCUREMENT OF AI BASED THREAT ASSESSMENT SOFTWARE

This document contains 54 pages including cover page and Appendices.

REGISTERED BY POST/BY HAND

Uttar Kaman Mukhyalaya
HQ Northern Comd (Signals Branch)
PIN- 908545
C/o 56 APO

6036/ Proj/ 2022-23 09 Feb 2023

To,

_____

_____

_____

(Vendor/ Institute concerned)

REQUEST FOR INFORMATION (RFI): FOR PROCUREMENT OF AI BASED THREAT ASSESSMENT SOFTWARE

1. The Ministry of Defence, Government of India intends to procure Artificial Intelligence based Threat Assessment which should be able to integrate legacy unstructured data available in different format and provide actionable intelligence by combining different databases through use of Artificial Intelligence and Data Analytics techniques.

2. This RFI for the Procurement of AI Based Threat Assessment Software consist of three parts as given below:-

(a) **Part I**. This part gives out the background AI Based Threat Assessment Software, the operational requirements, characteristic and features that should be met by the software. Important technical requirements that the software should fulfil are also mentioned within this part.

(b) **Part II**. The second part of the RFI states the methodology of seeking response from the vendors. Submission of incomplete response will lead to rejection and non-consideration of the same.

(c) **Part III**. This part lays down the guidelines for Framing Criteria for Vendor Selection/ Pre-Qualification in Buy Indian (IDDM), Buy (Indian), Indigenous Research & Development and Buy and Make (Indian) Cases.

3. **Liabilities of IA**

(a) This RFI is only a request for information about potential products/ services and no contractual obligation on behalf of Indian Army whatsoever shall arise from the RFI process. This RFI, on discretion of user, will be used for pre-qualification of suppliers for further issuing of Request for Proposal (RFP).

(b) **RFI Ownership**. All responses to the RFI will become the property of Indian Army and will not be returned.

(c) This RFI is issued as a means of technical discovery and information gathering.

(d) This RFI is for planning purposes only and should not be construed as a solicitation nor should it be construed as an obligation on the part of Indian Army to make any purchases.

(e) The Indian Army may utilize the results of this RFI in drafting a competitive solicitation (RFP) for the subject services/ products/ equipment.

(f) Any future contract that may be awarded must comply with Indian Army procurement requirements.

(g) This RFI is being issued with no financial commitment and the Buyer reserves the right to change or vary any part thereof at any stage.

(j) This RFI does not commit the Indian Army to pay any cost incurred in the preparation or submission of any response to the RFI.

(k) Participation in this RFI is voluntary and the Indian Army will not pay for the preparation of any information submitted by a respondent or for the Indian Army's use of that information.

(l) Buyer also reserves the right to withdraw the RFI, should it become necessary at any stage.

(m) Proposer of solution may be called to give a presentation to show his expertise in developing the solution.

4. **RFI Schedule**. RFI key dates are as given below:-

Start (In Days)	**End (In Days)**	**No of Weeks**	**Event**
N Day	-	-	Approved RFI hosted on website of MoD & Defence Procurement Portal
N+ 01	N+07	01	Vendor interaction at HQ Northern Command (Signals Branch) for clarification of any doubts on the issue of RFI.
N+08	N+15	01	Vendor interaction and final RFI responses from Vendors

N+16	N+25	01	Preparation of RFI Response Matrix and Comparative Analysis of Specification

PART – I

Intended Use of Artificial Intelligence Based Threat Assessment Software

5. **Problem Statement**.

(a) Indian Army operations require detailed Threat Assessment. Currently, details of Threat Assessment are available neither with Security Forces, nor other law enforcing agencies, however restricted information is available in the form of registers, both at Company Operating Base (COB) levels as well as with other Headquarters.

(b) Since the data is either non-existent or is recorded in legacy formats (documents & registers), no methods are available with SF for historic correlation of incidents due to which incidents cannot be tracked or predicted.

6. **Proposed solution**.

(a) An AI based networked solution that will enable storage and analysis of data to track and predict incidents.

(b) Details can be linked with national databases such as UIDAI, MoRTH in order to track vehicular move, as also monitor online presence of individuals including on Social Media platforms and derive linkages and patterns.

(c) Ability to import data available with other agencies within formation's Area of Responsibility (AOR) (legacy data available in Excel format).

(d) Enable central collation of details from various patrols. Real-time data visibility at all outstations (COB to Corps).

7. **Deliverables**.

(a) GUI based application for Desktop & mobile based platforms.

(b) Mob based application with Biometrics based identification of individuals to facilitate easy carriage by patrols. The application should enable RFID based tagging for cattle. RFID tags with embedded GPS chips can be designed, if possible.

(c) **Analysis Module**. To monitor physical move and recognition of locations.

(d) Integration with National Databases such as UIDAI & MoRTH. Import legacy databases available in excel format.

(e) Facial, Biometric correlation for humans-Move tracking through mobiles.

8. **System Design**.

(a) The software application is designed to integrate the Artificial Intelligent (AI) and Machine Learning (ML) aspects with the existing known datasets, thereby giving

the commanders and staff in chain a comprehensive and common picture as regards the operations, intelligence including the capability to carry out data processing in terms of staff checks, query management, utilization of business intelligence and visualization to arrive at courses of actions and also assist to rule out the less viable options. As the system is being planned keeping in mind the automation requirements of the Indian Army for intelligence generation, the system will be designed to exploitation by Artificial Intelligent (AI) and Machine Learning (ML) aspects.

(b) The software application is planned to be web based, capable of running on current, legacy as well as future hardware. The system design will allow development in modular and incremental manner addressing aspects of process automation such that sub systems/ modules can be strapped together to form the consolidated software. Further, Agile Methodology of software development is proposed to be employed in development of the same. The application is designed to be based on Centralised Architecture, being hosted on secured internet portal utilizing the envisaged infrastructure of CDCs and RDCs. Lastly, the system will be designed to handle classified data using commercial Software Encryption utilising secure network and other connected protocols.

9. **System Study**.

(a) The Developing Agency (DA) shall carry out a system study at User premises of various services that are running and the various applications to be integrated.

(b) The existing networking and data centre infrastructure available in the Army for hosting of the centralized application in order to provide optimal service assurance to the end users.

(c) As a pre cursor to the above, the DA shall interact with the users of the existing applications and then conduct an analysis for integration of these into the software.

Important Technical Parameters

10. **Scope**. The qualified DA shall be solely responsible for designing, development, integration, facilitating the testing and acceptance of a user friendly, fully functional software. The software should facilitate display and exchange of information over encrypted and secured internet connection. It should facilitate day to day functioning of operations and intelligence gathering and collating at various headquarters and also facilitate commanders in decision making by incorporating appropriate inputs. The scope of this project shall include but not limited to the following:-

(a) **Ingestion/ Collection of Data**. The application software should be able to ingest data as inputs from the application databases through API based integration/ offline integration (in case of legacy software/ incompatible format etc). Further the software application should be flexible to ingest data through manual feeding for data sets for which either data does not or newly defined data sets. The ingestion of this manual data will take place thorough independent modules to be designed and developed as part of the application.

(b) **Storage/ Population of Database**. The data received from various source application software should be populated in database only after time stamping the data for future conflict resolution in case of multiple instances of same / similar data. The database design should allow for addition, deletion and modification of new data sets, attributes and meta data fields in future. Any tampering pertaining to time stamp of data populated in the database has to be kept controlled and mitigated.

(c) **Collation and Corroboration of Data**. The database populated should be collated and corroborated based on information received from various sources. Information/ data sets for same and similar information/ data should be tagged and conflict resolution should carried out to populate updated information only. The manual override facility to accept cluttered / conflicted information should exist within the system.

(d) **Retrieval of data Query Management**. The data stored in the database should have meta data as per the laid down norms of Meta Data and Data Dictionary Standards. The database should be based on commercially available/ open source database with perpetual licenses and AMC. The database should cater for future migration to prescribed DBMS as per Indian Army/ Defense forces/ Government of India requirements. The query management should cater for spatial, temporal, keyword and attributes based queries. The system should support both structured as well as unstructured queries.

(e) **Visualisation**. The inputs from various software applications and manually entered data should be visible on OGC complaint platform. The output should confirm to user interface.

(f) **Analytics**. The data in the database should provide for discovering interpreting and communication significant patterns in data it should help the user see insights and meaningful data that the user might not detect otherwise. The data should be available for the purposes of pattern identification and pattern prediction and based on the same should cater for the generation of options at a later stage. The data and modules should not leave the system vulnerable to top AI / ML security threat like system manipulation, data corruption and poisoning, transfer learning attacks or data privacy breach.

11. Following are the Terms of Reference (ToR):

(a) Maximum use of Open Source Frameworks with assured support.

(b) Web Browser independence (if applicable).

(c) Google Material Design Document/ industry standard UI design document will be guiding documents for developing user interface and interactions.

(d) Maximum use of predefined data fields (dropdown menus, checkboxes etc) for input of data by users. Minimum data entry by users.

(e) Completely modular architecture such that any module can be replaced upgraded / added without affecting the functionality of other modules.

(f) Application wide comprehensive “natural language” based search facility.

12. A browser based solution is proposed to be developed. The solution should run on native browser with additional plug-ins that should be freely downloadable and should support Indian Army prescribed browsers. The capability to accept necessary upgrades has to be catered in the application for addressing compatibility issues with latest release of browsers. Additional plug-ins for running application on browsers have to be specified and have to be updated and vetted prior to implementation in the software. The application should be accessible on Windows/ Linux/ Android based machine and should accommodate for multiple levels of organization structure along with multiple layers of data processing capabilities including historical data.

13. **Data Migration**. The envisaged application should cater for data migration from other agencies/applications and build a fresh, authentic and clean database with logical separation of existing data. Necessary data cleaning of various fields is required to be carried out during migration of data. Necessary logic for addressing data migration with changed data structures/design in new database shall be addressed.

14. **Data Dictionary**. The vendor with assistance of the users compile a data dictionary of all data types used in the application and the same will be submitted both in hard and soft form as part of project deliverables.

15. **Data Security**. Adequate security measures will be ensured by the vendor as per the latest guidelines/ policies of Army Cyber Group (ACG) will be shared at appropriate time. Key security highlights are mentioned below:-

(a) Multiple levels of security should be incorporated, including object level security of repository, web level security of presentation catalogue, data level granular row/ column level access security, query limit security and user level security.

(b) **Multi Factor Authentication**. In order to ensure security and integrity of data, any transaction committed in the system should require multi-factor authentication as specified at the time of Supply Order

(c) Procedures and mechanisms will be developed by DA to prevent unauthorized access to the queries, reports and dashboards.

(d) The application security to be developed closely with the database security to ensure that all users having adequate application security can also have the access to the data in the database, i.e. application security and the database security to be mapped to each other for different profiles of users.

(e) Security authorization granted to the application users should be withdrawn once the access process is over.

(f) Access control methods to be implemented for the application.

(g) The application should undergo and pass the security testing by appropriate authority pre as well as post deployment. All existing security guidelines shall be implemented during the execution of project.

(h) The vendor will be responsible for fixing the observations raised by Army Cyber Group during the cyber vetting process in order to obtain security clearance. Any design change proposed by ACG at that time, due to detection of some previously unforeseeable vulnerability will be fixed by DA.

(j) Yearly Vulnerability Assessment, penetration test and necessary security upgrades are to be catered by DA during the Support (Warranty and AMC/ ATS) period.

(k) **Intrusion Protection System (IPS) and Intrusion Detection System (IDS)**. The IPS and IDS (Hardware/ Software) should be catered for in the security solution of the application software.

(l) The following security measures should be incorporated:

(i) Watermarking on all screens and printouts/ downloadable reports with details of user credentials and log in time.

(ii) Disabling Right click/ copy functionality.

(iii) Session Handling.

(iv) Disabling storage of Web pages at client end for office viewing.

(v) Audit records of all access, print, download etc. activities.

(vi) All inputs feeds have to be sanitized for use of special characters, unauthorised queries and symbols.

(m) Database Security like AES encryption for data at rest, secured backup, strict authentication and authorization mechanisms should be adopted.

16. **Suggested Security Aspects**. A few suggested security aspects to be implemented during various stages of software application development are given below:-

(a) **Design and Architecture**.

(i) The proposed software application should preferably be based on web based architecture wherein the client is able to access all functionalities of the system through the browser.

(ii) The application being developed should be based on the open standard and architecture.

(iii) Open Website Application Security Project (OWASP) cyber security vulnerabilities associated with website based application should be addressed.

(b) **Authentication and Authorization**

(i) Login only with a valid username and password.

(ii) Implementation of role based access control system.

(iii) Logging of all user activities and maintenance of audit trail with time stamping.

(c) **Session Management**.

(i) Once logged in, user session to be maintained as long as user is active.

(ii) Session timeout be defined in case of inactivity.

(iii) Server side state management techniques be used to ensure data entry.

(iv) Uniqueness of user session to be maintained throughout the system.

(d) **Input Validation**

(i) Validation of all user end data entry/ update to be implemented.

(ii) Use of data staging should be restored to for ensuring that users cannot address the main data base directly

(e) **Database Management**.

(i) **Database Design**. The database used within the application should be designed in a manner wherein it is able to cater to the maximum number of transactions envisaged within the application design

(ii) **Data Base Administrative (DBA)**. Techniques and methods for enabling DBA functionality should be incorporated within the application.

(iii) **Normalisation**. Databases deployed within the application should conform to BCNF Third Normal Form

(f) **Code Construction**. The coding language should be based on open standard and best practices for secure coding should be incorporated.

(g) **Data Encryption**. The security of data through all its stage i.e creation, transit, storage and destruction must be planned and implemented. Commercial/ industrial grade encryption like AES 256 bit may be considered for data encryption in initial phase and subsequent phase.

(h) **Communication Security**. The security of data during transit must be ensured. All communication between the client (browser) and the server must be through an encrypted channel (HTTPS). Implementation of TLS 1.2 or higher is recommended.

(j) **Error Handling and Logging**. All error/ exception be handled and logged for audit and analysis subsequently. Details of when and where the error occurred must be captured. Internal errors should not be displayed to the end user and generic error pages generated by the application should be used instead.

(k) **Website Security**. Threats like SQL inj, XSS, session hijacking, parameter manipulation, path disclosure need to be handled by implementation the relevant security features of the selected technologies.

(l) **Output Encoding**. To prevent Cross Site Scripting (XSS), all data used to render HTML or used for Java Script must be sanitized. CSRF mitigation should be enabled within the designed webpages.

(m) **Server Configuration**. The website server should be configured for the required security settings to ensure application pooling trust level, timeouts, SSl authentication. Default open ports must be blocked by restricting the associated services.

(n) **Security of Authentication Data**. Authentication/ user credentials stored within all database should be in an encrypted form. Users must be forced (through software design) to change default passwords at the time of initial login. Any default account existing within the database for housekeeping/ testing should be deleted/blocked explicitly.

(o) **Development Testing**. Individual modules of the application must be tested and followed by overall testing of the application must be carried with maximum load using test data to check the functionality and efficiency of the application.

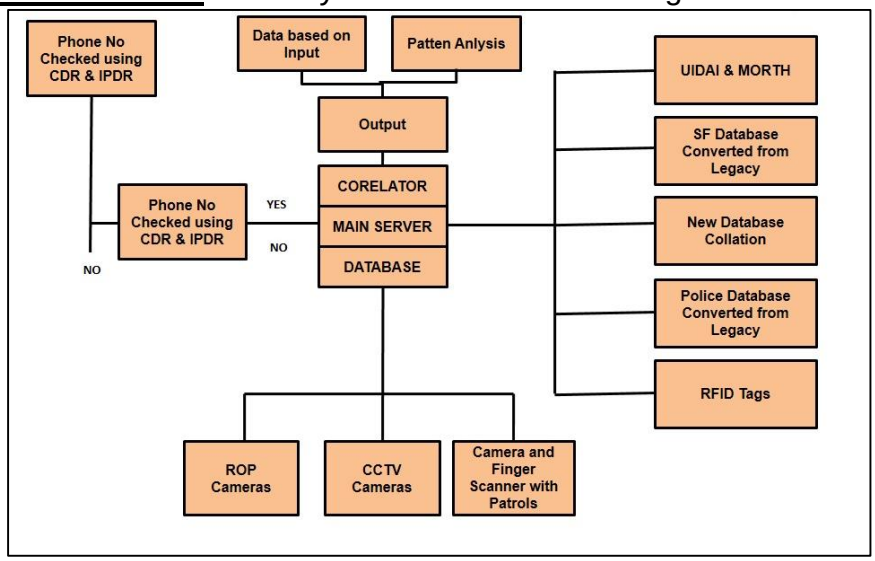
(p) **Bandwidth/ Network Integration**. Application should be designed in a manner wherein it is frugal in the use of scarce bandwidth resources.

(q) With the increase in data from open source as well as insider threats, it is imperative to incorporate a Threat Intelligence Platform and Extended Detection and Response (XDR) in the network architecture.

(r) **Cyber Security Vetting**. Post functionality testing by sponsor unit the software application along with the source code be forwarded to Army Cyber Group for undertaking detail cyber security vetting.

17. **Digital Signatures**. The system should have inherent capability for digitally signing any documents/reports/data produced as output. Only personnel authorized for specific function should be allowed to digitally sign the documents/reports. The system should maintain record of all such signing along with the signed documents.

18. **System Architecture**. The system architecture is as given below:



19. **System Scope**. In this project we intends to acquire big data analytical capability with the help of AI and ML which is capable of gathering required information from open sources that are available through all possible media, as well as taking into account and analysing structured and unstructured information that are made available as input from various sources. The proposed analytical tool should be capable of giving meaningful output as defined by the user from time to time. This project involves architecting, designing, developing, customizing, providing, installing and maintaining the big data analytics system for crime and terrorism intelligence for lifetime. Short listing the interested parties will be base on following broad criteria but not limited to following.

(a) Analysis of information from social media and other open system information.

(b) Structured and Unstructured Data Analysis.

(c) CDR & SDR Analysis.

(d) Voice Recognition.

(e) Metadata And GPRS (Mobile Intercepted) Raw Data Analysis.

(f) Analysis of CCTV Data (live and recorded) along with face recognition.

(g) Capability of Integration with other information system.

(h) Analysis of Data Extracted from Digital Electronic equipment using various extracting tools.

(j) Deep and Dark Web Analysis.

(k) Machine Learning models for smart analysis.

(l) Text mining models for various languages.

20. The end user will need a Digital repository based on big data analysis framework for investigation and intelligent analysis. The solution should have the following features :

(a) Establish a Digital Repository or Knowledge Bank for all Analysts for Collaborative Investigation across Location.

(b) Extraction and Ingestion of data from Deep and Dark Web and other sources such as local newspaper, social media, blog, forum website in order to ensure maximum coverage and understanding of patterns.

(c) Extract knowledge from diverse data.

(d) Strategic and Tactical Analysis requirement.

(e) **Geo Fence Analysis of Sentiment**. Users are able to view sentiment and post from specific geographical location over multiple period times.

(f) **Trending Discussion**. Users will be presented with a list of topics that are extensively being discussed across data sources such as news, blogs etc. This will provide insight into the needs and desires of the public.

(g) System should have inbuilt Text mining models for English, Hindi, Pasto, Arabic and Urdu languages.

(h) Multi-Format, Multi-Dimensional Link Analysis Tools for analysing Structured and Unstructured Information and provide 360 degree visualisation in one sight frame.

(j) Link Analysis of Investigation Data like Metadata, TDR, Individual and Group Associations, Incidents and Events, email Dump archive data.

(k) Capability to understand the Social Dynamics of the People Group/Network, i.e. the role played by individuals within a network.

(l) **Analysis of Historical Investigation, Intelligence and Analysis Reports**. System should have NLP(Natural Language Processing) models in English, Hindi, Pasto, Arabic, and Urdu languages to extract intelligence automatically from generated Reports, Intelligence Inputs, Open Source Documents and Memos. There can be several different types of reports and the system should have specific text mining algorithms for each of them.

(m) Video and Image Analytics for raw camera feeds from CCTV cameras, Social Media videos, images etc.

(n) **Data integration**. Continuously process entities extract from a huge number of document in order to establish the relationship of the entities and create profile in background. The extracted information can be queried instantaneously for finding the pattern needed to take investigation forward.

(o) Managing and organizing information for easy search and entity linkages.

(p) **Entity Extraction**. Support faceted free text search for any key-phrases or concept or theme to pin point all related entities.

(q) Customized dashboards for real time alerts and analytics.

(r) **Modular and Evolvable Data Architecture**. The modular and evolvable architecture supports incorporation of evolving inputs from various quarters. Constant research keeps the product up-graded and on the same page with the latest domain developments.

(s) Seamless intelligent analysis process and integration with multiple data applications.

(t) Solution capable of addressing majority of Analytical requirements of the organization.

(u) **Accelerate informed Decision Making**. Solution deliver to the user the desired visibility and real time intelligence to the decision maker to act upon sources.

(v) System should have inbuilt GIS for Geospatial intelligence, Timeline analysis for understanding the chronology of events, network graph to understand linkages, and provision to create charts and reports on the fly using a drag and drop function.

(w) **Preemptive Prediction and control of outcomes**. This will successfully prevent the crime itself from happening.

(x) **Alerts**. Analysts can define rules and thresholds in the application. When a rule is met, an alarm will be triggered in system and alerts will be sent to configured recipients. With in-app, email and SMS notifications, analysts will never miss an important event.

(y) **Communication and Response impact analysis**. Government often used social media platform to communicate idea and plan with the public. It is essential for official to measure the performance of the communication. The system measure the reach of communication, the no of comments, number of reports and the sentiment behind the comment.

21. **Actionable Intelligence**. The whole point of gathering and analyzing vast data is to produce intelligence, which enables analysts to make decisions with its help. Actionable with data, graphic and visual representations. Then, as additional human understanding intelligence converts data into contextual information, enabling real-time human interaction and judgment is further encoded into algorithms, actionable intelligence can be converted into machine-driven action, freeing the analyst to move onto the next anomalous finding, faster and with more confidence that the risk gap is being reduced effectively. Analyst can automate pattern analysis using historical and real-time data for finding anomalies' leading to automated actionable intelligence helping reduce time to detect, understand and respond by personnel.

Components

22. **Data Collection.** The system should be able to ingest and analyse huge amount of data including data from deep and dark web as well as internal structured and unstructured databases / documents available with the client.

23. **Data Processing.** The system should bring all disparate data sources into a single data model. The solution should run multiple algorithms on the data set for:

(a) Reducing Noise.

(b) Chunking documents to treat unrelated events separately.

(c) Self-learning Text Classification.

(d) Extracting themes out of data.

(e) Text Mining in English, Hindi, Pasto, Arabic, Urdu languages.

(f) Watch Words and alerts.

(g) Trends and Sentiments.

(h) Entity Disambiguation.

23. **Integration with GIS.** The tool should be integrated with a GIS platform to allow users to carry out their analysis on GIS. The GIS tool should be bundled with the solution.

24. **Analysis and Reporting**. The tool should be able to analyse various issues pertinent to intelligence organizations and should facilitate analytics and intelligence capabilities broadly summarized below:

(a) Search and generate reports for a person, place or organization of interest.

(b) Carry out entity extraction and entity disambiguation from the multiple data sources available with the client. Associate and cluster entities together.

(c) System should have inbuilt ML (**Machine Learning**) models for smart analytics. These models include but are not limited to clustering, classification, themes extraction, similarity etc.

(d) Identification and classification of inputs available with the organization to identify changing trends and sentiments which may pose a threat to law and order.

(e) Generate real time alerts.

(f) Perform Link analysis among people, organisations and places. Analyse perceived threat from received inputs.

(g) The data should be presented in user friendly formats such as reports, charts, graphs and maps.

(h) The system should carry out Geospatial intelligence and Timeline analysis.

25. **Client**. Server based scalable design architecture with Distributed Data Clusters, Virtualization and Hyper Converged Infrastructure embedded Hardware Architecture Set-up. Modules can be accessed by different entities, users from various locations and with high end data breach security controls by design.

Major Functionality

26. To collect intelligence input from different sources and build a centralized database for analysis and reporting, connects all frontiers and servers information at real time, centralization of disparate solution for key Data and Seamless Integration of Multi-Party system, Design and build a Central solution across complete hierarchy chain.

27. **Data Collection Layer**. The Data Collection layer should have the following features:

(a) Client gets a lot of data in the form of reports in word documents, excel sheets and other structured and unstructured datasets. The solution should be able to ingest all structured and unstructured data and automatically extract intelligence out of it.

(b) The solution should be able to ingest multiple documents, PDF’s, text files, zip, rar, mp3, mp4 etc at the same time. The system should have different text parsing and processing algorithms for each of the different types of reports available with client to extract maximum intelligence out of the reports. The system should identify and remove duplicates.

(c) The system should ingest all the Relational databases available with the client. The databases should be updated on a regular basis.

(d) The system should automatically convert all intelligence into Geospatial intelligence where available.

(e) The system should have a pipeline of RPA (Robotic Process Automation) modules to cleanse the data.

(i) The system should have modules to ingest:

(ii) CDR's and TDR's

(iii) Metadata

(iv) Interrogation reports

(v) Intelligence inputs

(vi) Reports

(vii) Extracted Mobile phone data

(viii) Data from Dark and Deep Web

(ix) News aggregates

(x) Other data sources available with the client

(xi) Audio and video

(f) System should treat different set of events within the same documents as different documents and extract intelligence from each of it separately.

(g) System should have pre-loaded datasets for Geospatial intelligence, local disturbances, and terrorism incidents.

(h) System should analyse intercepted mobile number raw GPRS data.

28. **Data Processing Layer**. The Data Processing layer should have the following features:

(a) System should have Trained Natural language processing algorithms for English, Hindi, Pasto, Arabic, and Urdu. The algorithms should have been trained on a supervised ML (Machine Learning) model.

(b) System should have models for text classification using supervised ML model. Any inputs by the end analyst should automatically cause the retraining of the model. The system should classify each event in one of the categories specified by the user.

(c) The solution should automatically carry out entity extraction from unstructured data sets including documents, excel sheets, presentations etc.

(d) System should extract all entities from unstructured data. The entities which need to be extracted have been defined as below –

(i) People
(ii) Organizations
(iii) Places
(iv) Events / Incidences
(v) Images and Videos

(e) System should extract and save themes from all unstructured data. The system should be able to form a conceptual and contextual understanding of all data.

(f) System should be able to carry out entity disambiguation from large datasets for people, locations and organizations.

(g) System should identify the tonality of the document for / against each extracted entity.

(h) System should have trained models for prompting the analyst on similar entities to what has been searched for.

(j) System should have trained models for recommending the next layers of searches based on the searches made by the analyst so far.

(k) System should allow the end user to create his own alerts. The alerts should be classified into specific threat classification priorities.

(l) System should have options to do “What-if” hypothesis.

29. **Data Storage Layer**. The Data Storage layer should have the following features:

(a) The solution should be able to analyze Peta Bytes of data. It should be able to hold as many documents as can be held in the database. The solution should be built on a Big Data Analysis framework such as Hadoop, MongoDb, and GraphDB etc. Any other Big Data analysis framework may be used as well.

(b) The system should bring disparate datasets into a single library.

(c) Solution should have support for any structured and unstructured data sets and should build indexes efficiently for easy search, discovery and analysis, using compaction and indexing techniques.

(d) It should be possible to add new data sources to the existing data repository for increasing the scope of analysis.

(e) The end analyst should be able to view the documents added (within the system) and add any entities that the text processing algorithms may have missed.

(f) The system should have a provision for parsing the data through a rule based module before storing it in the database to ensure accuracy of text processing modules.

(g) Data should be searchable using fuzzy matching, ranges, phrases and wild cards:

(h) Solution should have multiple searching algorithms including –

(i) **Fuzzy search**. For matching meta-tags and return a list of most likely correction of given words.

(ii) **Boolean Search**. Supported operators are AND, OR, NOT, XOR.

(iii) **Conceptual Search**. Enable searches to be processed and retrieved conceptually on the concepts against the article.

(iv) **Keyword Search**. Conceptually matches queries that consist of a single keyword. The system should stem the keyword, and identify documents that contain words that have the same stem as the keyword. Support all document formats.

(v) **Phrase Occurrence Search**. Should use a phrase occurrence search to find documents containing a range of occurrences of a phrase.

(vi) **Exact Phrase search**. Should allow querying with a term or a phrase in quotation marks, it should match them in their exact pre- stemmed form.

(vii) **Proximity Search**. Should look for documents where two or more separately matching terms occur within a specified distance, where distance is the number of intermediate words or characters. Proximity search goes beyond the simple matching of words by adding the constraints of proximity.

(j) The system should allow manual and fully automatic linking between related pieces of information, regardless of their format. The concept in document should be linked to those in another file. They can also be linked to related concepts within video or voice mail.

30. **GIS Platform**. The GIS Platform designed for the same should have the following functionality:

(a) Time series Data Analysis to visualize data changes over a period of time.

(b) User should be able to create multiple GIS views and compare them side by side.

(c) GIS Tools should be bundles within the solution as part of the same application.

(d) User should be able to superimpose multiple analytics on the same GIS View or create different (as many as required) views that may be needed.

(e) Analyst should be able to form clusters on GIS View.

(f) User should be able to search on GIS (by creating a Geofenced search box).

(g) User should be able to create his own points on GIS map.

(h) The software should have inbuilt maps from Open Street Maps. There should be an option to import maps in Tiff format.

(j) Every analyst should have a GIS view inbuilt inside the solution. User should be able to drag and drop data points on GIS.

31. **Analysis and Reporting.**

(a) System should support Boolean Queries.

(b) System should have a visual link analysis platform to:

(i) Study co-relation among people, places and topics

(ii) View link map of entities

(iii) Expand association

(iv) Zoom, pan, search and hide on maps

(v) Support different modes of representing networks such as hierarchical, cyclical etc

(c) System should support drag and drop functionality (for ease of usage) to take a network analysis on GIS and vice versa.

(d) User should be allowed to view the entity related document, the search entities should be automatically highlighted. Users should be allowed to mark new entities in the document on the fly.

(e) Should be able to generate a comprehensive view for each of the various entities including location, name of person, name of organization, keywords etc.

(f) Users can share their evidence, complete analysis along with their hypothesis with other users in the form of reports generated from within the system itself.

(g) Should be able to depict the relation between various extracted entities in a graphical form. The graph should be dynamic as clicking any link should open the relevant content.

(h) Investigators should be able to annotate reports, read and write comments/annotations on reports to aid in collaboration of work during investigative phase.

(j) Query templates should support entity based search and the time should be selectable on a timeline.

(k) Solution should have inbuilt modules for generating charts on the fly. The user should be able to choose a ‘X’ axis and ‘Y’ axis and choose the type of graphs (pie Graph, bar chart, line graph etc) which need to be generated

(l) Report generation module should be capable of generating reports based on query / result to include at least the following:

(i) Time / Date based query

(ii) Topics of relevance

(iii) Location base

(iv) Name of people / organization / group

(m) Information should be displayed using advanced visualization and charts.

(n) The solution should have support for Association, network, link, temporal and statistical analysis to help build a comprehensive analytical picture, revealing relationships, patterns and trends in data.

(o) Users should have option for identity resolution i.e. to merge similar entities into one entity and change the complete analysis based on then given hypothesis

(p) Users should be allowed to Group entities under one label.

(q) System should timeline analysis to view all events or chronology of an event on a timeline

(r) System should have provision to create a data shard for the generated query and be able to sort, filter or create pivots out of the data shard

(s) All locations should automatically be matched with the lat long of the respective location.

(t) All analytical views should be tightly integrated with each other i.e. the user should be able to make changes in one view and see the change reflect in all the other views (Geospatial, Timeline etc).

(u) The user should be able to drag and drop data from one view to another to see a detailed comprehensive view.

32. **Dark and Deep Web Monitoring and Analysis**

(a) Support for both Crawling and Scraping model as well as ability to ingest data from proprietary API's wherever available from the source end.

(b) Ability to Browser Based interactive scraping. This is for instances where there is a lot of Java Script based backend code and multilevel user interaction is mandatory.

(c) Ability to ingest data from multiple Social Media and Web platforms via their API’s (Application Programme Interface).

(d) Ability to provide input filters in the form of geographically bound polygon, multiple keywords, and Multiple Social media handles.

(e) The framework should be able to ingest data on real time basis from multiple RSS (Receive side scaling) feeds. The framework should be intelligent enough to manage the update frequencies to ensure the sanctity of data.

(f) The system should be able to extract information from Dark Web marketplaces

(g) The system should have specific ingestors to get data from local newspapers without any RSS feeds.

(h) System should be built on Big Data repository to handle large amounts of data.

(j) System should have complete provision for proper and optimized indexing mechanisms to ensure fast response to analytical queries.

(k) Database should be scalable enough to ensure fast insertion of high volume streaming data.

(l) Properly managed to ensure de duplication and optimized storage capacity usage.

(m) System should have inbuilt NLP capability to carry out entity extraction from unstructured data in the form of – People, Places, Events and Organizations.

(n) System should automatically calculate sentiment against a piece of text. Individual sentiment analytics should be done against entities defined in the text. The sentiment score can be carried out using a third party library over the internet.

(o) System should have capability to do Text processing in English, Hindi, Pasto, Arabic and Urdu language.

(p) System should classify every piece of text and extract themes out of it.

(q) System should carry out text summarization on the data inside the system

(r) User should be able to create views in the form of Geo Fenced data, Keywords or events and Persons.

(s) System should have a custom query builder to carry out Boolean operations.

(t) System should have multiple widgets and allow a user to create his own dashboard using any of the widgets available to him.

(u) Dashboard view should provide information in visually rich form factors in terms of Maps, Charts, Tag Clouds, Sort lists etc.

(v) Dashboard view should collate data from all sources relevant to user's analysis.

(w) Users should have option for a quick access time filter on a day, week and month basis.

(x) All analysis should be filterable by date range.

(y) All analysis should be filterable my multiple text filters.

(z) Filter data based on input keywords using multiple Boolean operations.

(aa) Option to use multiple search option in combination with each other.

(bb) System should give the user the capability to do Deep Dive analysis into each source separately

(ab) System should have an event calendar.

(ac) System should allow users to have multiple views in terms of trends, timelines, viral media, user views etc.

(ad) System should have flexibility to do timeline/temporal analysis to understand the flow of events.

(ae) System should have a link analysis module to understand the interrelations amongst many entities.

(af) System should have multiple reports for different platforms like user comparison, hashtag vitality, sentiment charts etc.

(ag) Multiple analytical containers should be sharable among users or should be provisioned.

(ah) System identifies Geo Locations (wherever possible) for user checking, pictures, tags, tweets etc.

(aj) System supports report generation in terms of graphs, documents, etc.

(ak) System supports Fuzzy search, Proximity search, Conceptual search on the gathered.

(al) System supports cascading query results i.e. subsequent queries should be possible.

(am) System support for analysis of GPRS interception data.

(an) System support for Contextual Analysis.

(ao) System has a link analysis module to identify common followers/ common following/ friends etc. of multiple profiles.

(ap) System should be scalable to add more Sources when available.

(aq) Should provide a full system and Subsystem health overview, alerting system technicians to servers that are down or to services that are running.

34. **Support of Software Products**. The DA will provide all necessary support to the licensed software products like compatibility with OS, middleware, antivirus etc. by regular updates/upgrades to the system as applicable and carry out necessary co-ordination with the OEM for support as desired from time to time. Further, entire support to open source software wherever used, if any, will be provided by the DA to include upgrade and update to address vulnerabilities and new functionalities. Strict version control with a record of change history and status to be exercised. Upgrades and updates provided by any third party agency will be required to be duly sanitised prior to deployment.

Development and Testing

35. Software will preferably be developed at user location however, if the same needs to be developed within DA premises, Non-Disclosure Agreement (NDA) and other connected security protocols should be adhered to. Hardware and software for the same will be provided by the vendor. Resources for carrying out this testing (viz. manpower for data entry, computers etc.) shall be provided by the DA. The software may also be tested (including Code Review) at any independent software testing agencies to confirm technical requirements including performance, security and reliability. Testing with respect to cyber aspects of all modules will be done by ACG to confirm implementation of security requirements. Acceptance after testing of each phase/module will be given by Indian Army HQ Northern Command.

36. Testing shall also include ease of installation, user friendliness, management and security and coding methodology besides adherence to the functional requirements in the SRS. DA shall be responsible for documentation of testing.

37. Getting the developed software tested will be the responsibility of the DA as per the SRS. It will be tested by Independent third party software tester. The cost of testing will be borne by the vendor.

38. No remote testing of software under development will be done on internet without the approval of Indian Army.

39. **Establishment of System Integration Test Facility (SITF)**. The DA will establish a fully functional SITF in the User premises. SITF will have a prototype Test Bed which will be used for system simulation, development, testing of software configuration controls, information security measures, facilitate evaluation of cost and benefit of technology insertion based on user feedback.

40. **Training**. DA should provide training to persons of units/ formations at designated locations, after delivery of each phase deliverables. Sufficient technical hands who understand the package should be formed into adequate number of training teams which can simultaneously execute this task at desired locations.

Maintenance and Support

41. **Maintenance**. Suitable tools shall be developed to provide dash boarding facilities to important functionaries, for data import/export, data synchronization, data conversion and disaster recovery to facilitate the integration process.

42. **Help and Support**. The DA shall be responsible to provide support to the end users after the rollout of the application. This shall include registration of tickets as both online and offline mode (telephone/ email).

43. The DA should provide support for the developed application by the means of warranty/ATS. The desired details are as given in succeeding paragraphs.

44. **Warranty**. The DA will provide free maintenance and warranty support from the date of final acceptance and shall be deemed to have expired only after successful negotiation of maintenance support package is concluded between user representative and the DA. The date of issuing the final acceptance certificate would be deemed to be the date on which the warranty will commence. All issues arising from application will be addressed by the DA at no additional cost. In case the issue noticed within the warranty period persists beyond end of warranty period, the same will be addressed by the DA in ATS period without any additional cost. Further, support during warranty period will include: -

(a) Analysis and bug fixing when notified.

(b) The database maintenance.

(c) Enhancement, if required by the user within the scope of the SRS and also any additional major/minor process change/enhancement, if required so as address any policy change.

(d) System training support along with requisite training artefacts and user support materials, fully updated to reflect any changes carried out in the software, to cater for roll-over of personnel on a quarterly basis at user end.

(e) Provisioning regular monthly/quarterly patches on physical media as a clean single step executable.

(f) Regular presence / availability within reasonable time, of software engineers of the vendor for solving any problem.

(g) Periodical data base management/maintenance.

(h) Yearly Vulnerability Assessment, penetration test and necessary security upgrades.

(j) Periodic security clearance/ clearance after any change in the package from ACG.

45. **Post Warranty Annual Tech Support (ATS)**. Depending upon the relevance of the technology used in development and exploitation of the application after three year warranty period, a new contract under PAC for ATS of software will be initiated at the discretion of user. All the warranty clauses, bug fixing and modifications required during ATS after expiration of warranty would be catered for free during ATS along with any additional changes needed during ATS period due to policy change/ user feedbacks. However, vendors can quote their rates for ATS as part of their commercial offer as per **Appendix A**.

46. **Proprietary Rights**.

(a) The DA will be required to give an undertaking that the proposed development and customization would in no manner be a violation of Intellectual Property Rights (IPR) of any software and that the Indian Army would not be responsible towards any legal fallout at a later stage. The customized software developed including subsequent versions would become a proprietary item of the Indian Army after final acceptance of the software after testing. Indian Army reserves the right to prepare any number of copies for distribution, use/ modify the code in any other project. Similar terms apply to the documentation, User manual and training materials including presentations, which will be used by the vendor during the training phase.

(b) The following will be the requirements for incorporating IPR provisions:

Ser No	Artefact	Associated IPR	Remarks
(i)	System Design	System Patent	System in entirety
(ii)	Functional features	Methods Patent	Number and listing of functions performed by software
(iii)	External appearance	Registration of design	GUI menus

(iv)	Input domain	Registration of design, Patent	Data type, format, source
(v)	Processing Algorithm	Method Patent	Algorithms
(vi)	Compilation script	Copyright	Code specific to OS and compiler
(vii)	Source Code	Copyright	Code in a programming language
(viii)	Libraries/DLLs/ Executables	Copyright/ Licenses	The artefact sharing for re-use
(ix)	Logos/Images/ Audio files	Copyright/ Licenses	All audio files, images developed for buyer

47. **Supply of Source Code**. The entire source code of the software will be provided after each iteration. The final source code for the software will be provided with proper documentation (Software Product Specifications design document etc.) explaining the functions of each module/ routine etc. Necessary instructions for incorporating any modification/changes in the software and its compilation into executable/installable product will be explained clearly in the documentation itself. All source code will become a proprietary item of the Indian Army. It must be understood that the software will be developed for the Army as a dedicated project.

48. **Software Development Center**. The DA has to have a software development center in India. If they do not have a software development center it should be willing to have one after allotment of the contract.

49. The DA are required to follow the procedure for response as explained in **Appendix 'B'** of this document. In addition, the DA are required to furnish details as per Performa at **Appendix 'C'**. The vendor must furnish answers to the Questionnaire as given at **Appendix 'D'**.

50. DA should confirm that the following conditions are acceptable:

(a) The solicitation of offers will be as per "Single Stage-Two Bid System". It would imply that a "Request for Proposal" would be issued soliciting the technical and commercial offers together, but in two separate sealed envelopes. The validity of commercial offers would be at least 18 months from the last date of submission of offers.

(b) The technical offers would be evaluated by a Technical Evaluation Committee (TEC) to check its compliance with the RFP.

(c) The application software of all TEC cleared vendors would be put through a trial evaluation on a "No Cost No Commitment" basis. A staff evaluation would be carried out to analyse the result of field evaluation and shortlist the application software for introduction into service.

(d) Amongst the vendors cleared by staff evaluation, a Contract Negotiations Committee (CNC) would decide the lowest cost bidder (L1) and conclude the appropriate contract.

(e) The DA would be bound to provide product support for the time period specified in the RFP, which includes spares and maintenance tools, jigs and fixtures for field and component level repairs.

(f) The vendor would be required to accept the general conditions of contract given in the Standard Contract Document.

(g) Offset (if applicable). Not applicable.

(h) **Integrity Pact**. An integrity pact alongwith appropriate IPBG is a mandatory requirement in the instant case.

(j) **Non Disclosure Agreement (NDA)**. This RFI and its questionnaire is sensitive in nature. The vendor is required to sign a NDA for the same. The format for the NDA is given at **Appendix 'E'**.

52. **Indigenous Content (IC)**. It is pertinent that maximum development of the software should be with indigenous software (certification by the Statutory Auditor of the Bidder that the software has been developed within India) driving the desired applications while the backend software i.e. Operating Systems continues to be OEM defined. The self certification by the Bidder and certification by the statutory auditor of the Bidder shall certify that the software has been developed within India. If an Indian Bidder acquires the sole ownership of a proprietary software by way of acquisition/one-time buy-out or any similar means and becomes the sole owner of Intellectual Property Rights (IPRs), such software can be considered as indigenous to the extent of the value of its utilization in the current contract, provided an undertaking is given that the Seller shall maintain the ownership of the software throughout the contract period.

PART II

Procedure for Response

53. Vendors must fill the form of response as given in **Appendix 'B**'. Apart from filling details about the company, details about the exact product meeting other generic technical specifications should also be carefully filled. Additional literature on the product can also be attached with the form.

54. The filled form alongwith softcopy in a CD should be dispatched to the address given at Para 3 of **Appendix 'B'**.

55. Last date of acceptance of filled form is **24 Feb 2023**. The vendors short listed for issue of RFP would be intimated.

56. The Government of India invites responses to this request only from Original Equipment Manufacturers (OEM), Authorised Vendors or Government Sponsored Export Agencies (applicable in the case of countries where domestic laws do not permit direct export by OEMs). The end user of the equipment is the Indian Armed Forces (IA). A copy of the response is also to be shared with Department of Defence Production (DDP) by the firms for updating the competency map of the firm held with DDP.

57. **Vendor Parameters**. The vendor should be a registered company in India. It should have a registered office, Operations and Maintenance support team in India. The OEMs of the proposed product and services must also have their registered office, operations, maintenance and repair infrastructure in India. The vendor and the OEMs must be technically competent, financially sound and should have adequate infrastructure to set up, maintain and support the proposed networks as per following criteria:-

(a) The vendor and OEMs should have a strong financial base. Balance sheets and Profit/ Loss statements for the past three years should be submitted, clearly highlighting the annual turnover.

(b) Vendor and OEM should have a well-established base and technically competent maintenance and repair facility to maintain the network. The vendors should submit the support and repair escalation matrix along with maintenance methodology as asked in the RFI with additional details as relevant.

(c) Vendor shall confirm that that he shall be signing copy of all agreement with OEMs/ Sub vendors for execution of the Turnkey solution to deliver the desired SLAs which will be discussed with user and submitted to the user and on conclusion of the same. OEMs shall also confirm that the proposal has been well communicated to them and that they comply with the requirements as projected in the RFI or later (RFP, Contract/ any other time) during all clarifications given before the issue of RFP.

(d) Vendor must confirm that there are no Patent/ legal issues that might become hindrance in implementation of the solution at later stages.

(e) Must highlight and obtain the Government clearances as applicable.

58. Vendors should confirm that the following conditions are acceptable:-

(a) The solicitation of offers will be as per “Single Stage-Two Bid System”. It would imply that a ‘Request for Proposal” would be issued soliciting the technical and commercial offers together, but in two separate sealed envelopes. The validity of commercial offers would be at least 18 months from the date of submitting of offers.

(b) The technical offers would be evaluated by a Technical Evaluation Committee (TEC) to check its compliance with RFP.

(c) The equipment of all TEC cleared vendors would be put through a trial evaluation at a suitable location nominated by the buyer on a “No Cost No commitment’ basis. A staff evaluation would be carried out by SHQ to analyse the result of field evaluation and shortlist the equipment for introduction info service.

(d) Amongst the vendors cleared by GS evaluation, a Contract Negotiations Committee would decide the lowest cost bidder (L1) and conclude the appropriate contract.

(e) Vendor would be bound to provide product support for the entire life span of the communication grid network with IoMT sensor grid, which includes technical support, spares and maintenance tools/ software.

(f) The vendor would be required to accept the general conditions of contract given in the Standard Contract Document as per DPM.

(g) An integrity pact along with appropriate IPBG is a mandatory requirement in the instant case.

59. **Procedure for Response**.

(a) Response to RFI will be submitted at under mentioned address :-

Uttar Kaman Mukhyalaya
HQ Northern Comd (Signals Branch)
PIN- 908545
C/o 56 APO

(b) In addition to providing details about company, details about the exact product meeting other generic technical specifications should also be carefully filled. Additional literature on the product can also be attached with the form.

(c) Last date of intimation of willingness to participate and acceptance of filled form (Appendix) is six weeks from date of issue of RFI.

(d) A vendor interaction may be conducted with all interested parties subsequent to receipt of proposal. Exact date and time of the vendor interaction will be intimated to all companies who intimate their willingness to participate.

60. The Government of India invites responses to this request only from Indian Vendors who have tie ups with Original Equipment manufacturers (OEM)/ Authorised Vendors/ Government Sponsored Export Agencies (applicable in the case of countries where

domestic laws do not permit direct export by OEMs). The end user of the equipment is the Indian Armed Forces (name of user service).

PART III

GUIDELINES FOR FRAMING CRITERIA FOR VENDOR SELECTION/

61. The guidelines prescribed for short-listing/ pre-qualification of Indian vendors are enumerated in the succeeding paragraphs. Paragraph 62 deals with the parameters that may be considered for short-listing of vendors, whereas Paragraph 63 amplifies the process for applying selection parameters to the process of Vendor Short listing.

62. **Parameters**.

(a) **General Parameters**

(i) Applicant Entity should be an Indian Vendor

(ii) Business dealing with applicant Entity or any of its allied entities should not have been suspended or banned, by MoD/ SHQ or any Government Department or organization (as defined in Guidelines for Penalties in Business Dealings with Entities issued vide Ministry of Defence, D (Vigilance) MoD ID No 31013/I/2006-D(Vig) Vol II dated 21 Nov 2016). None of the Promoters and Directors of applicant entity should be a willful defaulter.

(iii) “Entities” will include companies, with whom the Ministry of Defence has entered into, or intends to enter into, or could enter into contracts or agreements. (iv) “Applicant entity” may be a company, subsidiary, an associate company (as defined in the Companies Act, 2013) a consortium or a Joint Venture (JV).

(b) **Technical Parameters**

(i) Vendor shall be a software developing entity or a software integrator of defence equipment, Academic Institute and not a trading company, except in cases where the OEM participates only through its authorized Vendors.

(ii) Minimum two years" experience in broad areas of software development/ integration of software applications in the instant procurement case. If not, then cumulative experience of at least three years in above areas, resulting in gaining of competence for manufacturing the proposed application software.

(iii) Where product involves integration, previous experience of not less than one year/ one project in integration of software/ applications shall be required.

(iv) **ICT Cases**.

(aa) Certification to be included if linked to scope of work – Gartner Quadrant/ ISO 9001/ CMMi 5 or more (specifying development/ service/ acquisition models)/ ISO 27001. For Information Security and large value projects preferably CMMi 5 may be specified.

(ab) Compliance with IEEE/ ITU standards depending upon nature/type of project or solution required.

(ac) Academic Institute of repute.

(c) **Financial Parameters**

(i) Average Annual Turnover. Minimum average annual turnover for last three financial years, ending 31st March of the previous financial year i.e 31 Mar 2022 may please be informed.

(ii) Net Worth. Net worth of entities, ending 31st March of the previous financial year i.e 31 March 2022 may please be informed.

(iii) Insolvency. The entity should not be under insolvency resolution as per Indian Bankruptcy Code at any stage of procurement process from the issuing of RFP to the signing of contract.

(iv) Credit Rating (Desirable Financial Parameter). Long term credit rating equivalent to CRISIL rating on Corporate Credit Scale as CCR-BBB or better, and SME-04 or better for SMEs issued by credit rating agencies recognized by SEBI. Credit rating should be as on 31st March of the previous financial year i.e 31 March 2022.

(d) **Other Parameters**

(i) Industrial License (IL). Details of valid defence industrial license with a copy to be enclosed by the vendor.

(ii) Registration. Details of registration.

63. **Stipulations for Applying Parameters**

(a) Areas like software development/ development of APIs/ Software integration etc.

(b) In case the Applicant Entity is unable to meet the Financial Parameters by itself, it may rely on its Holding Company (as defined in the Companies Act, 2013 and amendments thereof) (“Companies Act”) for fulfilment of the Financial Parameters, in which case reliance must be placed on the Holding Company towards fulfilment of ALL the Financial Parameters.

(c) In case the Applicate Entity is unable to meet one or more of the Technical Parameters by itself, it may rely on a Group Company (ies) for fulfilment of the Technical Parameters. A Group Company in relation to the Applicant entity may be:-

(i) A company of which the Applicant Entity it is an Associate Company. Such company should have ownership, directly or indirectly, of at least 26% of the voting shares of the Applicant Entity.

(ii) A company which is an Associate Company of the Applicant Entity. The Applicant Entity should have ownership directly or indirectly, of at least 26% of the voting shares of such Associate Company.

(iii) A company with whom the Applicant Entity is commonly owned, directly or indirectly, for at least 26% of the voting shares by another company. For example: An Applicant Company A is an Associate Company for Company B, in which B holds at least 26%. Further, C is also an Associate Company of B, in which B holds at least 26%. In this case the Applicant Company may use the credentials of C as well.

(iv) The Holding Company and Subsidiary Companies (as defined under the Companies Act) of the Applicant Entity.

(d) The Applicant entity may be a single entity or a group of entities (the “Consortium”), coming together to implement the project. In such case:-

(i) The credentials of only those members or their related entities may be counted, who have at least 26% equity stake in the Consortium.

(ii) Each Consortium should have a designated Lead Member.

(iii) For Technical Parameters, any of the Consortium members or their Group Companies may meet the criteria.

(iv) For financial Parameters; the Turnover and Net Worth of the Consortium Member shall be reckoned proportionate to Consortium Member"s equity stake in the Consortium, and each Consortium member should meet the other criteria pertaining to Insolvency and Credit Rating. In case the Consortium Member relies on its Holding Company for any one of the above-mentioned Financial Parameters, then reliance must be placed on the Holding Company for meeting all the financial parameters.

(e) Vendors should provide all necessary self-authenticated documentation in support of their achievement of criteria. Such documentation should inter-alia include:-

(i) Details of projects/ supply orders successfully executed in the last two years.

(ii) Annual reports for three years of applicant entity, parent and associate companies, consortium and JV partners.

(iii) Details of shareholders, promoters, associated, allied and JV companies.

(iv) Details of vigilance action, viz. ongoing investigation and suspension/debarment/blacklisting actions against the applicant entity or any of its allied entities, parent company or consortium and JV partners, if any by any Department/agency of Central Government.

(v) A certificate from CA/ CS indicating the financial parameters for the last three years as per Paragraph 60 (c).

(f) Any vendor furnishing false information will be liable for action as per existing guidelines.

Appendix A
(Refer to Para 45 of Part I of RFI)

COMMERCIAL OFFER

1. **Price Bid Format**. The Price Bid Format is given below and vendors are required to fill this up correctly with full details. The bid should take into account all features as demanded and as recommended by the vendor.

2. **Development Cost**.

S/No	Activity	Cost	Tax (%)	Total Cost
(a)	Cost of Software Development (all tax inclusive)			
(b)	Cost of training per personnel per location			
	Total Cost			

3. ATS for Maintenance of the software and providing upgrades as required after the free warranty period of three years: -

S/No	ATS For	Cost	Tax (%)	Total Cost
(a)	1st Year			
(b)	2nd Year			
(c)	3rd Year			
(d)	4th Year			
(e)	5th Year			
(f)	6th Year			
(g)	7th Year			

Company Seal (Common Seal of the Company)

Company name: (**Authorised Signatory of Company**)

Date:

Note: - All prices quoted should be landed cost inclusive of all taxes, duties etc

Appendix B
(Ref to Para 50 of Part I of RFI)

REQUEST FOR INFORMATION: PROCEDURE FOR RESPONSE

General

1. The Indian Army is planning to design and develop Threat Assessment Software. With the view to identify probable DAs who can undertake the said project, OEMs ,Authorised Vendors and Academic Institutes are requested to forward information on the product which they can offer. The parameters and broad specifications of the item are mentioned in the questionnaire attached as per Appendix 'A'. In addition, the vendors are required to furnish details as per Performa at Appendix 'C'.

2. Apart from the information sought in the Appendices, the vendors may also forward technical details, product brochures and literature etc pertaining to the item in question.

3. The required information/ details may please be forwarded to the following address by 24 Feb 2023.

(a) **Uttar Kaman Mukhyalaya,**
HQ Northern Comd (Signals Branch)
PIN- 908545
C/o 56 APO

(b) **Head Quarter 16 Corps (Signals Branch)**
PIN- 908516
C/o 56 APO

Appendix C
(Ref to Para 50 of Part I of RFI)

VENDOR INFORMATION PROFORMA

1. **Name of the Vendor/ Company/ Firm**. (Company profile including Share Holding pattern, in brief, to be attached).

2. **Type (Tick the Relevant Category)**.

Original Equipment Manufacturer (OEM)	Yes / No
Authorised Vendor of foreign Firm	Yes / No (attach details, if Yes) Others (give specific details)
Academic Institute	Yes/ No

3. **Contact Details**.

(a) Postal Address :
(b) Building No :
(c) City :
(d) State :
(e) Pin Code :
(f) Tele :
(g) Fax :
(h) URL / web Site :
(j) Email :

4. **Local Branch / Liaison Office / Agent (if any)**

(a) Name :
(b) Postal Address :
(c) Building No :
(d) City :
(e) State :
(f) Pin Code :
(g) Tele :
(h) Fax :
(j) URL / web Site :
(k) Email :

5. **Financial Details. Category of Industry (Large / Medium / Small Scale):**

_____

6. **Certification by Quality Assurance Organisation**.

Ser No	Agency	Certification	Applicable from (Date and Year)	Valid Till (Date and Year)
(a)				
(b)				

7. **Details of Registration**

Agency	Registration No	Validity (Date)	Equipment
GeM			
DGQA/ DGAQA/ DGNAI			
OFB			
DRDO			
Any other Govt Agency			

8. **Membership of FICCI/ ASSOCHAM/ CII or other Industrial Associations**

Ser No	Name of Organisation	Membership Number
(a)		
(b)		
(c)		
(d)		

9. **Equipment/ Product Profile (to be submitted for each product separately)**

(a) Name of Product:

(IDDM Capability be indicated against the product) (should be given category wise for e.g all products under night vision devices to be mentioned together).

(b) Description (attach technical literature) :

(c) Whether OEM or Integrator :

(d) Name and address of Foreign collaborator (if any) :

(e) Industrial License Number :

(f) Indigenous component of the product (in percentage) :

(g) Status (in service / design and development stage) :

(h) Production capacity per annum :

(j) Countries / agencies where equipment supplied earlier (give details of quantity supplied) :

(k) Estimated price of the equipment :

(l) Alternatives for meeting the objectives of the equipment set forth in the RFI.

(m) Any other relevant information :

10. **Declaration**. It is certified that the above information is true and any changes will be intimated at the earliest.

(Authorised Signatory)

Appendix D
(Ref to Para 50 of Part I of RFI)

REQUEST FOR INFORMATION: QUESTIONNAIRE

1. **Vendor Information**. The vendor will provide the following information:-

(a) Name of person responsible for the information contained in this RFI.

(b) Telephone Number, Fax Number, Email address, Web page.

(c) When was company established?

(d) Have your implemented your system in Army for any operational role? If so, please provide reference information?

(e) Development center. Location (s) of the nearest company location and its distance to Delhi as well as the hours of operation and support.

(f) A sample implementation schedule for a solution implemented in government/ public sector organization.

(g) Describe any third party alliances, relationships, or dependencies.

(h) Please provide information on your implementation methodology.

(j) What documentation is provided with the software/ system and in what format?

(k) Was your software written by your organization or acquired from a third party?

Operational Parameters

2. **System Concept**. The background, system concept, system design, architecture, deliverables and the proposed service employment of application software and its utilization have been covered in detail. The vendor is required to clearly indicate suitability and validate the design and architecture of the application software.

3. **System Concept**. The application is to be designed and developed as web based hardware agnostic software and the hosting, automation and data visualisation alongwith OGC complaint GIS platform is required. The vendor is required to clearly indicate suitability and validate the same.

4. **System Design and Architecture**. The vendor is required to validate the integration of the application with existing data sets. The vendor would also be required to respond to the development of software as modular/ incremental model and the methodology/ approach to achieve this.

5. **System Study**. As mentioned in the referred Para the vendor will list out the requirements pertaining to the knowledge/ information required of existing applications including various technical parameters like existing networking protocols, storage, bandwidth availability, databases be used, various formats being used to generate output and any other related technical/ non-technical information.

6. **Important Technical Parameters**.

Q No	Questionnaire	Response
1.	Will the solution be able to ingest multiple documents, PDF's, text files etc. at the same time and match them with critical databases like CCTNS, Dial 100 etc to aid intelligence and decision making?	Yes / No
2.	Will the solution be able to pull in data from Social Media and new sources?	Yes / No
3.	Will this application support for both Crawling and Scraping model as well as ability to ingest data from proprietary API's wherever available from the source end?	Yes / No
4.	Will the system have ability to Browser Based interactive scraping? (This is for instances where there is a lot of Java Script based backend code and multilevel user interaction is mandatory)	Yes / No
5.	For Social Media data, will the system have an ability to provide input filters in the form of: (a) Geographically bound polygon (b) Multiple Keywords (c) Multiple Social Media Handles	Yes / No
6.	What mechanism will the system use for scraping data from Social Media and related sources?	Answer briefly
7.	How will the system get data from different sources including Twitter, Facebook, News Media?	Answer briefly
8.	How will the system support for full time stack of Twitter REST API to extract extended information?	Answer briefly
9.	Will the application support for scraping based Facebook data extraction to get access to FB data that is hidden from Graph API?	Yes / No
10.	Will the application support for handling and creating multiple FB avatars to ensure scraping?	Yes / No
11.	Will the application support for scheduling these FB avatars scraping periods and frequencies?	Yes / No
12.	Will the application support for doing precision FB crawl by specifying or assigning Avatars to specific profiles or groups?	Yes / No
13.	Will the system have provision to monitor people profiles in Facebook?	Yes / No
14.	Will the system have a provision to identify suspicious profiles on Facebook based on users likes?	Yes / No

15.	Will the system be able to ingest and analyse data from WhatsApp?	Yes / No
16.	Will the system should accept documents in Batch and real time mode?	Yes / No
17.	How will the application integrate with Video Analytics framework deployed across the city & focus on cameras in areas where crime rate is trending?	Answer briefly
18.	Will the system cater to complex and innovative use cases?	Yes / No
19.	Will the application be able ingest data from multiple open source databases available with the client?	Yes / No
20.	Will the system work if databases are updated on a regular basis?	Yes / No
21.	Will the system integrate with public and non-public data sources and create a 360-degree view of the ecosystem?	Yes / No
22.	Will the framework be able to ingest and correlate data on real time basis from multiple RSS feeds?	Yes / No
23.	Will the framework be intelligent enough to manage the update frequencies to ensure the sanctity of data?	Yes / No
24.	Can the system have modules to ingest/integrate doubtful data sources with: (a) Interrogation reports (b) Intelligence inputs (c) FIR's (d) Travel related information (e) Crime related information (f) Other data sources available with the client such as vehicles	Yes / No
25.	Will the solution be able to analyse Peta Bytes of data (Unstructured and Structured)?	Yes / No
26.	Can the solution be built on a Big Data Analysis framework such as Hadoop, MongoDb, GraphDB, etc or a combination of two or more such frameworks?	Yes / No
27.	Can the system be using capabilities from such architectures to create one holistic solution?	Yes / No
28.	Will the system be able to perform in-depth analysis on the ingested unstructured data and provision for analytics with respect to future events and social media activities?	Yes / No
29.	Will the system have complete provision for proper and optimized indexing mechanisms to ensure fast response to analytical queries?	Yes / No
30.	Can these indexes be stored and reference able in the system?	Yes / No

31.	How can the Database be scalable enough to ensure fast insertion of high-volume streaming data?	Yes / No
32.	How will the system seamlessly integrate with streaming sources?	Yes / No
33.	Can the streamed data be analysed in a real time fashion?	Yes / No
34.	Can the system bring disparate datasets into multiple libraries and link them to base intelligence on top of the architecture?	Yes / No
35.	Can the solution support for any structured and unstructured data sets?	Yes / No
36.	Will the system build indexes efficiently for easy search, discovery and analysis, using compaction and indexing techniques?	Yes / No
37.	Will the searched elements be available for all kinds of analysis offered by the framework?	Yes / No
38.	Will the user be able to configure alerts for any new update on their key analysis?	Yes / No
39.	Will it be possible to add new data sources to the existing data repository for increasing the scope of analysis?	Yes / No
40.	Can the new data sources be added and plugged to generate new analysis or build upon existing modules?	Yes / No
41.	Will the solution automatically carry out entity extraction from unstructured data sets including documents, excel sheets, presentations, etc.?	Yes / No
42.	Can the system extract the following entities from unstructured data (indicatively) – (a) People (b) Organizations (c) Places (d) Events / Incidences (e) Images and Videos (f) Dates and Timelines, and more	Yes / No
43.	Can the system have provision for entity disambiguation?	Yes / No
44.	Will the solution form a conceptual web of understanding post extraction of meaningful snippets of data from text heavy documents?	Yes / No
45.	Can the solution provide insights across large documents in human understandable form and ready for further analysis?	Yes / No
46.	Will the solution classify documents and events in specific categories?	Yes / No

47.	Will the classification models be self-learning and trained on client's datasets?	Yes / No
48.	Will the training of the models be incremental in nature and the System Integration be able to ensure operational efficiency on those models?	Yes / No
49.	How will the system automatically calculate sentiment against a piece of text?	Yes / No
50.	Can Individual sentiment analytics be done against entities defined in the text?	Yes / No
51.	Can the sentiment score be carried out internally and not using a third-party library over the internet?	Yes / No
52.	Can the system classify every piece of text and extract themes out of it?	Yes / No
53.	Can the system automatically relate or link multiple documents whereas files in different formats can be linked to each other?	Yes / No
54.	How can the data be searchable using: (a) Fuzzy Search (b) Boolean Search (c) Conceptual Search (d) Keyboard Search and Stemming (e) Phrase Occurrence Search (f) Default Phrase Search (g) Exact Phrase Search (h) Proximity Search	Yes / No
55.	Can the system allow manual and fully automatic linking between related pieces of information, regardless of their format?	Yes / No
56.	Can the System support Boolean Queries?	Yes / No
57.	Can the System have a visual link analysis platform to Study co-relation among people, places and topics?	Yes / No
58.	Can the System have a View link map of entities?	Yes / No
59.	Can the System have an Expand association?	Yes / No
60.	Can the System have a Zoom, pan, search and hide on maps?	Yes / No
61.	Can the System have a Support for different modes of representing networks such as hierarchical, cyclical etc?	Yes / No
62.	Can the module be integrated with video analytics features of the framework to cull out real time insights?	Yes / No

63.	Can the link analysis allow the user to create different business rules for entities and relationships to create a more understandable graph?	Yes / No
64.	Will the link analysis have capabilities like clusterization to simplify the graph?	Yes / No
65.	Will the system have graph theory implementation to identify paths/connections between nodes separated by multiple degrees of separation?	Yes / No
66.	Will the system have ability to ingest data from multiple Social Media and Web platforms via their API's and integration with link analysis platform in-built with the tool?	Yes / No
67.	How will the System support drag and drop functionality (for ease of usage) to take a network analysis to any other kind of analysis?	Yes / No
68.	How will the User be allowed to view the entity related document and how will the search entities be automatically highlighted?	Yes / No
69.	How will the users be allowed to mark new entities in the document on the go?	Yes / No
70.	How will the application be able to generate a comprehensive view for each of the various entities including location, name of person, name of organization, keywords, etc.?	Yes / No
71.	How can the Users share their evidence, complete analysis along with their hypothesis with other users in the form of reports generated from within the system itself?	Yes / No
72.	Will the system have flexibility to do timeline/temporal analysis to understand the flow of events?	Yes / No
73.	Will the System have a link analysis module to understand the interrelations amongst many entities?	Yes / No
74.	Given an extremist target profile, will the system be able to suggest similar profiles based on parameters including but not limited to facial recognition based identical profile picture, similar network linkages, sharing same ideology?	Yes / No
75.	Will the system be able to depict the relation between various extracted entities in a graphical form?	Yes / No
76.	Will the system be able to depict the relation between various extracted entities in a graphical form?	Yes / No

77.	Will the user be able to annotate reports, read and write comments/annotations on reports to aid in collaboration of work during investigative phase?	Yes / No
78.	How will the query templates support entity-based search and will the time be selectable on a timeline?	Answer briefly
79.	Will the system have the ability to detect objects such as weapons in the images using Deep Learning based models?	Yes / No
80.	Will the solution have inbuilt modules for generating charts?	Yes / No
81.	Can the report generation module also be capable of generating reports based on query / result to include at least the following: (a) Time/Date based query (b) Topics of relevance (c) Location based (d) Name of people/organization/group	Yes / No
82.	Can the user be able to generate reports in the form of : (a) Area (b) Events or crimes (c) Persons	Yes / No
83.	Can the information should be displayed using advanced visualization and charts?	Yes / No
84.	Can the system have multiple widgets and allow a user to create his own dashboard using any of the widgets available to him?	Yes / No
85.	Can the dashboard view be modified to provide information in visually rich form factors in terms of Maps, Charts, Grids, Sort lists etc.?	Yes / No
86.	Will the dashboard view collate data from all sources relevant to user's analysis?	Yes / No
87.	Will the dashboard be able to depict varied kinds of analysis in single dashboard with docking features?	Yes / No
88.	Will the users be able to access dashboards based on time and date filters?	Yes / No
89.	Will all analysis be filterable by date and multiple other ranges?	Yes / No
90.	Can all the analysis be filterable my multiple text filters?	Yes / No
91.	Can user Filter data based on input keywords using multiple Boolean operations?	Yes / No
92.	Will the use have option to use multiple search option in combination with each other?	Yes / No

93.	Will the system give the user the capability to do Deep Dive analysis into each source separately?	Yes / No
94.	Can all locations automatically be matched with the lat-long of the respective location?	Yes / No
95.	Can the system be able to carry out comprehensive network analysis between entities?	Yes / No
96.	Can the system be able to identify types of associations parallelly?	Yes / No
97.	Will the system offer Drag and drop functionality with respect to exporting grid elements to the graph?	Yes / No
98.	Will the system be able to Dynamically update the details to be shown along with a particular node of the graph?	Yes / No
99.	Will the system allow selective expansion of nodes for in depth analysis?	Yes / No
100.	Will the system have inbuilt AI based threat models to identify suspect social media profiles prone to extremism and radicalization?	Yes / No
101.	Will the system identify people on social network based on mail ID, phone numbers etc.?	Yes / No
102.	Will the system identify trends, key influencers against a particular event or a 360-degree profile of an event, organization, individual or a location? Can several other entities be amalgamated into it?	Yes / No
103.	Will the system allow the user to cluster similar types of nodes?	Yes / No
104.	Will the system allow the user to create sub-graphs from a bigger graph?	Yes / No
105.	Will the system be able to find out the shortest path and different paths from one entity to another?	Yes / No
106.	Will the system be able to link people, organizations, events and locations along with phone numbers, account numbers, money involved, related documents, etc.?	Yes / No
107.	Will the system show the properties of the nodes and relationships in detail?	Yes / No
108.	Will the system allow the user to write additional rules and scenarios on entities and relationships?	Yes / No
109.	Will the nodes and relationships be available in different views like timelines and GIS?	Yes / No
110.	Will it be possible to search the entities and relationships within the graph?	Yes / No

111.	How can the graph thus created be exportable to different formats (word, excel, grid, maps, files, etc)?	Answer briefly
112.	Can the graph offer visualizations in different forms (tree form, hierarchical form, etc.)?	Yes / No
113.	How can the system provide a full logging system to audit all user activities taking place inside the system?	Answer briefly
114.	Can the system have a Web and mobile application where the operators will feed in inputs coming from sources such as Wireless, ROIP etc.?	Yes / No
115.	Can the application be customizable where further fields may be added after studying the type of inputs received by the department?	Yes / No
116.	Can the web and mobile application be made for ease of use and fulfil all the requirements of the end user?	Yes / No
117.	Will the Web and Mobile application have set-up masters to manage key fields of information collected through forms?	Yes / No
118.	Can the masters be configurable and can it be managed by System admin?	Yes / No
119.	Can the Web Application have form based information reporting i.e. Data entry users can add new incidents through guided forms with defined fields which tag the data entered respectively?	Yes / No
120.	In the web application will the user be able to edit information entered before final submission?	Yes / No
121.	In the Web application the users will not be able to edit entered form without appropriate privileges?	Yes / No
122.	How can we make web and mobile application form entry simple and easy to use?	Yes / No

7. **Generic Queries on the Application Software**.

(a) How do you plan to implement strict relationship constraints in the database and how will you achieve balance between normalization and performance?

(b) How do you plant to execute spatial, temporal, attribute, predefined words, structured and unstructured?

(c) **Data Exchange**. The vendor is required to list out different file formats for exchange of data with legacy systems, other systems and databases. The additional file formats proposed for ingestion, storage, collation, retrieval, visualization, analytics and dissemination of data should also be listed out.

(d) **Data Entry**.

(i) What validation procedures/ process does the vendor proposed to identify the data/ critical data elements which require validation during the development process?

(ii) How does the vendor propose to achieve the validation through role based access control for various data entry personal?

(e) **Database Management**.

(i) How does the vendor proposed to replicate the database to prevent loss of data due to any reason?

(ii) What procedures (software or other) does the vendor propose to ensure security of the database?

(iii) What technique will the vendor utilized for data visualization and transfer of data on the network?

(f) **Database Administration**.

(i) How does the vendor propose to achieve change of super admin, admin and user creation, deletion, modification and grant of role based access?

(ii) How does the vendor propose to execute table management in the database and manage access rights in tables?

(g) **Data Migration**. What techniques/ procedures do you propose to facilitate data migration from other agencies/ applications and build a fresh, authentic and clean database with logical separation of existing data?

(h) **Data Dictionary**. How does the vendor propose to create/ compile a data dictionary of all types of data and enable the user to also create a new data dictionary entry through a UI or any other technique?

(j) **Data Security**. The vendor is required to give out a comprehensive security solution for the security of data at rest and while in transit. The proposed solution should align with the latest guidelines/ policies of ACG. The Virtual Desktop Infrastructure (VDI) provided for vetting should have source code in debug mode and role wise authentication details with password to ease out the vetting process. The vendor should also include any other aspects related to security which he plans to include for a comprehensive security solution for the application software.

8. **Suggested Security Aspects**.

(a) **Designed and Architecture**. What are the latest technological solutions available for design of an application software. Will the proposed web based architecture be a sufficient solution for the Indian Army. The security aspects related to web based architecture and the client server model should be included in the response.

(b) **Authentication and Authorisation**. What procedure/ techniques do you propose for implementation of authentication, authorization and role based access control for users? Is latest procedures/ techniques to implement this should be included in the response.

(c) **Session Management**. How does the vendor plan to manage the session and maintain the uniqueness of the session? The server side state management techniques should also be included in the response.

(d) **Data Encryption**. How does the vendor propose to provide security of data through all its stages i.e creation, transit, storage and destruction? Will the vendor be able to use SAG approved encryption algorithms for data encryption. If yes, kindly inform the detailed methodology.

(e) **Code Construction**.

(i) What type of coding language is proposed to be used?

(ii) Software coding standards being complied may please be given out.

(f) **Communication Security**. How does the vendor propose to implement security of data during transit?

(g) **Error Handling and Logging**. The technique/ procedure for handling of errors and logging the same should be included in the response.

(h) **Website Security**. How does the vendor propose to website security?

(j) **Server Configuration**. The vendor should clearly bring out the required security settings to ensure application pooling trust level, time outs, SSL authentication and other sever configuration related security issues and their solutions.

(k) **Development Testing**. Will the vendor be able to get the individual modules of the application tested with maximum load using test data to check functionality and efficiency of the application?

9. **Application Administration**. How does the vendor propose to provide an enterprise level administrator system and other administrators at various level. How will the administrators work in delegate and decentralized manner?

10. **Rights and Role Base Access**. How does the vendor propose the management of roles and rights through software frontend?

11. **Vertical and Horizontal Scaling**. How does the vendor propose to achieve vertical and horizontal scaling of the application software through the hierarchy of IA.?

12. **Digital Signatures**. How does the vendor propose to implement digital signing of documents, reports and data produced as output and maintain a record of the same? The digital signature should be enable/ disable as per the role based access control.

13. **Audit Trail**. The application software should have the capability of self-test and diagnose the problems if any. The audit must be enabled to be initiated by admin/ super

admin besides a periodic audit and the report should be generated. How does the vendor propose to achieve this?

14. **Support of Software Products**.

(a) The vendor should provide details of life cycle support, version management and builds of application software. The time period/ frequency of patches/ updates and the ways and means to push the updates should be listed out as response to this RFI.

(b) The mechanism of pushing the updates till end user has to be brought out clearly.

15. **Development and Testing**. Is the software application design, development, coding, testing and implementation an iterative process? Can the same be achieved by fixed GSQRs? Are regular interactions with user/ planner necessary? How much effort do you envisaged to be involved in minor/ major tweaking and course correction (if required) of the application software.

16. **Establishment of SITF**. The vendor should clearly respond to the requirement for establishing a SITF for testing of application software. The proposed testing criteria/ methodology should also form a part of the response.

17. **Training**. The vendor will indicate the ability and willingness to offer following:-

(a) Training to persons of units/ formations at designated location after delivery of the product.

(b) The vendor will indicate the facilities available at OEM/ Vendor premises to conduct training. He will also give out how he can assist in carrying out training of user and maintenance personnel.

(c) Recommended training period for users and maintenance will give out by the vendor.

(d) Training aggregates for conduct of training like projection systems Technical Literature, Brochures and Computer Based Training (CBT) packages.

(e) Availability and willingness of the vendor to provide soft and hard copies of user handbook, technical manuals along with the CBT for training should be indicated.

(f) How does the vendor plan to provide a separate training mode functioning will be provided at any level irrespective of Normal Mode.

18. **Maintenance and Support**. The vendor will details provide details of the following:-

(a) Guarantee/ warranty.

(b) AMC.

(c) Monthly/ Quarterly Patches.

(d) Periodic database management maintenance.

19. **Post Warranty ATS**

(a) ATS philosophy of the OEM.

(b) What the level of ATS envisaged for minimizing downtime.

(c) Will special tools be provided for carrying out error correction and detection?

(d) **Cost per year**. Is it the same for all subsequent years? If not then rate of change per year may clearly be given out.

20. **Mean Time between Failure (MTBF) and Mean Time to Repair (MTTR)**. MTBF and MTTR of the application software will be indicated by the vendor.

Manufacturing and Production Aspects

21. **Experience**. The vendor will indicate the number of years of experience. Details of any similar project executed by the vendor to supply such equipment to any entity in India and abroad may be provided.

22. **Research, Development and Manufacturing Facilities**. The vendor will provide details of all R&D manufacturing infrastructure in India and abroad.

23. **Indigenisation**. The vendor will give out his ability and willingness to supply the product to meet the requirements of Buy Indian (IDDM) and/ or Buy Indian to meet the aim of Indigenisation as per provision and spirit.

24. **Infrastructure Requirements**. The vendor will give details of the following:-

(a) Minimum requirements of hardware and software.

(b) Recommended requirements of hardware and software.

(c) Requirements for future scaling.

(d) The OS on which the software will be able to run.

(e) Development environment proposed to be used.

25. **Software Capability & Requirements**. The vendor will give details of the following:-

(a) Will the application software integrate with active directory?

(b) Will the application software facilitate the setting of thresholds and provide alerts to users.

(c) Can user easily create these thresholds and alerts?

(d) How are these alerts communicated to the end user?

(e) Name all browsers that your system will be compatible with.

26. **Quality Control**. The vendor will give details of the following:-

(a) CMMi level certification.

(b) IEEE certification.

(c) ISO certification.

(d) Security certification.

(e) Any other certification.

(f) Quality control and software testing fools and methods used during development.

(g) Third party testing.

27. **Integration**. The vendor will give details of the following:-

(a) Number of data sources that can be simultaneously accessed.

(b) Type of data sources supported

(c) Name all third party products required to meet the criteria described in this RFI.

(d) Does your system provide APIs?

28. **Actions Before Software Development**. The vendor will give details of the following:-

(a) Analysis and details of applications to be integrated and connected requirements.

(b) Method of integration of modules.

(c) Software Requirement Specification (SRS) and vision documents.

(d) Process mapping methodology.

(e) Workflow management methodology.

(f) Use of SDLC methodology.

(g) Software modules and function point analysis/ effort estimation.

29. **Actions During Software Development**. The vendor will give details of the following:-

(a) Modules of Ops, Int, OL and other additional packages proposed to be developed.

(b) Features envisaged to be provided for ease of use.

(c) Interfacing applications/ agencies.

30. **Actions After Software Development**. The vendor will give details of the following:-

(a) Installation procedure.

(b) Scalability.

(c) Reliability.

(d) Extension/ Flexibility.

31. **Terms and Conditions**. The vendor will give details of the following:-

(a) Handing over of Intellectual Proprietary Rights (IPR).

(b) Supply of source code.

(c) Delivery, Installation and implementation schedule.

(d) Support services.

(e) Transition.

(f) Production.

(g) Performance.

32. **Detailed Cost Model**. The vendor will give details of the following:-

(a) Estimate of scoped requirements.

(b) Is there anything that would require an additional or third part purchase to meet the requirements outlined in this RFI?

(c) What is your expected product life cycle?

(d) What is your licensing model and prices?

(e) Method used for cost estimation.

33. **Detailed Cost Model**.

(a) Estimate of scoped requirements.

(b) What is included?

(c) It there anything that would require an additional or third party purchase to meet the requirements outlined in the RFI.

(d) Support offered. (Hours, methods of contact)

(e) What is your annual maintenance?

(f) What is your licensing model and price?

(g) Method used for cost estimation.

(h) Assumptions.

34. **Miscellaneous**.

(a) Is there a requirement of preparation of DPR?

(b) Recommended categorisation as per DPR.

(c) Recommended development of software time plan.

(d) Requirement of PSQR prior to formulation of GSQR.

(e) Is there any requirement of PoC.

(f) Time required for training of persons on software.

35. **Timelines**. The vendor should clearly bring out the proposed development cycles for the software with clear cut milestones of each cycle.

36. **Method of Implementation**. The vendor should clearly bring out the most optimum and fast process for implementation of the project. The vendor is required to bring out the proposed approach for implementation of the project in order of priority i.e all “BUY’ and “MAKE" approaches.

37. **Evaluation**. The vendor is required to list out methods proposed for evaluation of offered solution. The vendor should also define the bare minimum acceptable scalable model for evaluation.

Appendix E
(Ref to Para 51(j) of Part I of RFI)

NON DISCLOSURE AGREEMENT

This Non-Disclosure Agreement is entered into by and between SHQ/MoD (Disclosing Party) and _____located at _____ (Receiving Party) for the purpose of preventing the unauthorized disclosure of confidential information as defined below. The parties agree to enter into a confidential relationship with respect to the disclosure of the RFI for procurement of the Project.

1. For purpose of this Agreement, “Confidential Information” shall include all information or material in which Disclosing party is engaged. If confidential information is in written form, the Disclosing party shall label or stamp the materials with the word “Confidential” or some similar warning. If confidential information is transmitted orally, the Disclosing Party shall promptly provide a written communication indicating that such oral communication constituted confidential information.

2. Receiving party shall hold and maintain the confidential information in strictest confidence for the sole and exclusive benefit of the Disclosing party. Receiving party shall carefully restrict exercise to confidential information to employees, contractors and third parties as is reasonably required and shall require those persons to sign Non-Disclosure restriction atleast as protective as those in this Agreement. Receiving party shall not, without prior written approval of Disclosing party, use, publish, copy, or otherwise disclose to others, or permit the use by others or to the detriment of Disclosing party, any confidential information. Receiving party shall return to the Disclosing party any and all record, notes and other written, printed or tangible materials in its possession pertaining to confidential information immediately if Disclosing party requests it in writing.

3. Nothing contained in this Agreement shall be deemed to constitute either party a partner, joint venture or employee of the other party for any purpose.

4. If any provision of this Agreement is held to be invalid or unenforceable by court of law, the remainder of this Agreement shall be interpreted so as best to effect the intent of the parties.

5. This agreement expresses the complete understating of the parties with respect to the subject matter and supersedes all prior proposals, agreements, representations and understandings. This Agreement shall not be amended except with the written consent of both the parties.

6. That in case of violation of any clause of this Agreement, the Disclosing party is at liberty to terminate the services of Receiving party without assigning any reason and shall also be liable to proceeded against in a Court of Law.

7. This Agreement and each party‟s obligations shall be binding on the representatives, assigns and successors of such parties. Each party has signed this Agreement through its authorised representatives.

Disclosing Party

_____ (**Signature**)

_____ (**Typed or Printed name**)

Date _____

Receiving Party

_____ (**Signature**)

_____ (**Typed or Printed name**)

Date _____