HARDWARE AND SOFTWARE LICENCES TECHNICAL SPECIFICATIONS

Contract title : Consolidation and Further Development of the Judicial Communication and Information System

Publication reference: EuropeAid/136-166/DH/SUP/Bal Tender No: EC/BiH/TEN/14/022

Column 1-2 should be completed by the Contracting Authority

Column 3-4 should be completed by the tenderer

Column 5 is reserved for the evaluation committee

Annex III - the Contractor's technical offer

The tenderers are requested to complete the template on the next pages:

- Column 2 is completed by the Contracting Authority shows the required specifications (not to be modified by the tenderer),
- Column 3 is to be filled in by the tenderer and must detail what is offered (for example the words "compliant" or "yes" are not sufficient)
- Column 4 allows the tenderer to make comments on its proposed supply and to make eventual references to the documentation

The eventual documentation supplied should clearly indicate (highlight, mark) the models offered and the options included, if any, so that the evaluators can see the exact configuration. Offers that do not permit to identify precisely the models and the specifications may be rejected by the evaluation committee.

The offer must be clear enough to allow the evaluators to make an easy comparison between the requested specifications and the offered specifications

Lot 1 – Implementation of Business Intelligence in B&H judiciary

All courts and prosecutors' offices in BiH collect large amounts of data from case proceedings and their business operations. To keep track of the data, courts and prosecutors' offices need to use a wide range of software programs, such as MS Excel, MS Access and different database applications like Case Management System (CMS). For that purpose an ICT tool - Business Intelligence (BI) Software needs to be introduced to the judicial information system. Business intelligence system represents integrated and complete approach of support to business decision making, which converts huge amounts of data to the information, from which the knowledge is generated, that eases the decision making in order to generate additional business value.

Implementation of the business intelligence system will make periodic reporting and monitoring of the work performance of judicial institutions easier. By providing statistical reports it will contribute to the automation of data quality control process.

The BI system will significantly aid the decision-making process. Relevant stakeholders will have adequate reports accessible in real time enabling them to monitor the process of resolving of all cases (including war crime cases) and steer strategic and operational decisions towards achieving improved judicial efficiency.

Main prerequisite for proper functioning of the BI is that the data warehouse, which is the actual storage of the data needed for the BI, contains good quality data. As part of this activity certain reports, checks and alert will be created and implemented as standardized reports in the BI. These reports will ensure that the person responsible for the data quality in judiciary institution can analyze the data in question and to act to ensure correction of the data on the daily basis.

With the implementation of the data warehouse HJPC will be able to provide more detailed historization of the data, i.e. with the advance modelling of the data warehouse it will provide necessary flags to identify the data which was valid at certain point of time.

This project includes implementation of module for advanced business reporting and establishment of required data warehouse i.e. Business Intelligence Solution (BI) and Data warehouse solution DWH)

Subject of this lot include following:

- Software license for DWH data base with partitioning option

- Software platform for BI tools and respective licenses

- Implementation of BI and DWH solutions

- Implementation of "near-live" data quality system on standby database

- Integration of BI reports with the judicial portal

- Preparation and delivery of documentation for implemented solutions

- Education and training of advanced users (read-write and administrator users)

Beneficiary (HJPC BiH) will provide necessary hardware based on IBM AIX 7.1 OS with 1 CPU (2 cores), 64 GB RAM, fiber channel connection for implementation of DWH solutions BI solution. In case that the offered hardware platform is not compatible with proposed solution contract is required to include hardware platform with same or better specification as part of the overall solution. Also, beneficiary will provide 2 processor licenses for Oracle Weblogic Suite 11g R1 for application server for implementation of BI solution web server(s) in active-active mode. If proposed solution is not certified to be implemented on Oracle Weblogic 11g then the contractor needs to include web server with same or better specification which must be able to provide active-active clustering.

Business Intelligence (BI) solution must be able to provide at least three different level of access namely:

- read-only for minimum 150 users - accessing the predefined reports and dashboards (multiple reports combined in single page or tabbed pages)

- Read/write for minimum 20 users - which will be able to create contents (reports, graphs, dashboards, KPI etc.)

- Administrator rights for minimum 1 user – administer all BI solution objects (data-marts, repositories, users, reports, etc.)

Proposed BI solution must be scalable in both directions number of users (additional 250 read-only users and 20 read/write users) and number of application server to ensure unrestricted growth of BI platform.

Item No	Specifications	Qty	Specifications Offered	Notes, remarks, ref to documentation	Evaluation Committee's notes
1.1	Implementation of data warehouse - Database software for data warehouse and Data Warehouse Database Management must support and provide following: - database sizes greater than 100 TB , - should enable access to database with GUI and SQL clients, - more than 500 columns in row, - tables size greater than 30 GB, - capabilities like union, intersect, except, join (left, inner, outer, right, merge), - referential integrity, - transactions, - temporary tables, - materialized views or equivalent, - partitioning based on data range, - row level locking, - expression and full-text indexes,	1			

Item No	Specifications	Qty	Specifications Offered	Notes, remarks, ref to documentation	Evaluation Committee's notes
	- common data types (integer, char and/or varchar, decimal, string, date/time, etc.) - programming options (cursors, triggers, functions, stored procedures) - Database software for data warehouse must support management from Oracle Enterprise Manager 12c - Database software for data warehouse must include data partitioning and backup options - Database solution for warehouse must be compatible with Symantec Backup Exec 12 and/or Symantec NetBackup enterprise 7.5 and up - Data warehouse design must be done by automation tool for data warehouse creation which can provide easy insight into design of data warehouse and can be used to make any future changes to the data warehouse model - Data warehouse management tool must possess meta-data repository as part of the tool which will be used for saving ETL procedures, versioning of data mappings, recycling of deleted object, data about data structures, etc. - Meta data repository data warehouse management tool should				

Item No	Specifications	Qty	Specifications Offered	Notes, remarks, ref to documentation	Evaluation Committee's notes

	include full export and backup option for saving the ETL/DWH model
	
	- Data warehouse design should include creation of all entity relationship diagrams
	
	- Data warehouse must be created in line with the BI solution prerequisites i.e. to be formatted in line with dimensional model based on two types of data grouping: dimensions and fact tables in form of star schema
	
	- All dimensional tables beside columns required by subject areas must have following fields:
	
	  o unique key
	
	  o source reference code – unique key related to source system
	
	  o date valid from – date from which row is effective
	
	  o date valid to – date until which row is effective
	
	  o other column(s) which is/are recommended/required for better performance of data warehouse and/or BI system
	
	- All record in dimensional tables have to be historised i.e. (tracking changes in dimensions over time) by implementing Slowly Changing Dimensions (SCDs) type 6 methodology				

Item No	Specifications	Qty	Specifications Offered	Notes, remarks, ref to documentation	Evaluation Committee's notes
	- Data preparation schema will contain all data extracted from the different source systems with detailed log of data which was extracted - Extract, Transform and Load procedures must be executed sequentially with detail log on execution timeline and with possibility to restart at certain point in sequence if the execution halts at certain point - Extract procedure will transfer all data from core systems which was created and/or modified in period from last extraction with detailed log per each source system with amount of data extracted - During data transform part error validation must be implemented. All records with validation errors will be moved to separate schema and alert will be raised and information regarding the data errors need to be delivered to mail recipient with relation to source of the data (point of data creation) - Data which passed the data validation process will be loaded to live and test data warehouse schema in renormalized form - Auditing on execution of ETL procedures must be implemented in the way that detailed data (start time, end time, processed record number, number of bad records, etc.) on				

Item No	Specifications	Qty	Specifications Offered	Notes, remarks, ref to documentation	Evaluation Committee's notes
	execution of each separate procedures should be kept - Detail information on completion of all ETL procedures along with number of records processed and time taken must be delivered to system administrators via email - Data warehouse solution must be able to enforce different levels of security and access to all and /or any part of the data warehouse solution so that users get access to object that he is authorized to access				
1.2	Implementation of Business Intelligence (BI) solution - Business Intelligence must support and provide following: - possibility to create highly formatted, printable and interactive reports and dashboards i.e. dynamic response to change of parameters and/or addition of new fields on principle of drag-and-drop, - ad hoc reporting/ querying of data source i.e. users should be able to add/remove columns and filter data according to their needs from the predefined data stores, - provide support for integration with mobile devices (not part of this implementation but should support possible future development),	1			

Item No	Specifications	Qty	Specifications Offered	Notes, remarks, ref to documentation	Evaluation Committee's notes
	- should provide possibility to provide geospatial analysis and reports i.e. reports and dashboards based on the geographical location of data, - OLAP (Online analytical processing) processing to enable users to drill-down thru data marts in order to get more detail analysis, - possess metadata management to enable users to reuse metadata models for similar analyses and/or similar reports and dashboards, - includes the visual development tools to enable users to manipulate with all elements of the reports and dashboards, - end of use for business user i.e. business user will use "drag-and-drop" functionalities to shape reports and dashboards, - Business Intelligence solution should be able to provide uninterrupted access to minimum 350 simultaneous users in various modes (administration, read, read/write, etc.) - BI platform should be able to install on IBM Power6 machines or compatible hardware with minimum of 4 CPU 64 GB RAM, 2 x 250GB HDD or better specification should be included in solution				

Item No	Specifications	Qty	Specifications Offered	Notes, remarks, ref to documentation	Evaluation Committee's notes

	- BI should be certified to work (creates content and access the BI content) from within following internet browsers:
	
	   o Microsoft Internet Explorer, version: 9.x and up (required)
	
	   o Mozzila Firefox, version: 13.x and up
	
	- BI platform should be compatible with existing Oracle Weblogic server or minimum 2 processor licenses for compatible web server should be included in BI solution
	
	- BI platform should be from same vendor or compatible to work with software for database which will hold the warehouse data and where the BI metadata will be saved
	
	- BI platform should be able to execute the reports requests on the server side instead of the client side with data caching on the server
	
	- BI platform should have possibility to access various types of data sources (RDBMS, SQL queries, Excel files, flat files, etc.)
	
	- BI platform should enable access to the BI content from various portable devices (smartphones, tablets, etc.)				

Item No	Specifications	Qty	Specifications Offered	Notes, remarks, ref to documentation	Evaluation Committee's notes
	- BI platform must have module for creation, modification, publishing of reports for interactive panels/dashboards - BI tool for creation of the reports should be intuitive, based on drag-drop reports creation methodology, ability to perform various filtering, formatting, custom formula creation, parameter definition, several report viewing options, easy graph creation on exiting report, direct report print/data export, saving parts of analysis (filters, parameters, formatting, etc.) for future use - BI platform should support export of reports in several formats and should by default support PDF, XLS, HTML, RTF, CSV - BI platform should poses mode/tool/module to create, define parameters, security and publish reports based on the BI data model - BI platform must include module/application/tool for ad-hoc analysis which can be parameterized and published on interactive panels/sites/dashboards (collection of ad-hoc analysis which grouped on one page and published to specified users) - BI interactive panels/sites/dashboards must poses "security system" which will be implemented on user level i.e. each				

Item No	Specifications	Qty	Specifications Offered	Notes, remarks, ref to documentation	Evaluation Committee's notes
	user should only see data that he is authorized to see - Creation of the interactive BI panels/sites/dashboards should be limited to specific users (minimum 20 users) while other 150 users will only have ability to change predefined parameters and refresh data on interactive panels/sites/dashboards - BI platform should be able to automatically run specified reports and based on the predefined ranges perform specific actions (KPI validations etc.) and deliver the alerts to predefined responsible persons for review - Alerts from the BI platform should be delivered over various communication protocols (live on the user interface, email, mobile devices, etc.) - BI platform should enable access to the BI content from various portable devices (smartphones, tablets, etc.) - BI tool should enable direct/indirect integration with Microsoft Office for presentation of reports or direct queries - BI platform must include tool for administration of all components of the system (starting/stopping server,				

Item No	Specifications	Qty	Specifications Offered	Notes, remarks, ref to documentation	Evaluation Committee's notes
	manipulation of the BI content and definitions of the BI presentation level and data marts, management of users/group privileges on BI objects) - BI platform must be able to restrict the amount of data transferred from server to client (number of rows, cell, etc.) in order to maintain good performance - BI platform must possess security mechanisms to separate access levels on the BI content (reports, dashboards, etc.) and to enable restricting row level data aces based on the data to which user is authorized to access - BI platform must be able to integrate into existing Active Directory infrastructure for the user authentication and group access. Users will be placed in specified group in Active Directory which will enable them to access the BI content				

Item No	Specifications	Qty	Specifications Offered	Notes, remarks, ref to documentation	Evaluation Committee's notes
	ANCILLARY SERVICES for LOT 1:				
	- The contractor must install, configure, test and put into operation all software components for data warehouse (Item 1.1) and for business intelligence solution (Item 1.2) in HJPC premises				
	- If existing Oracle Weblogic application server is used contractor must install Business intelligence platform in active-active cluster to ensure high availability otherwise if new application server is used it also must be configured in active –active mode on minimum two servers with possibility to add new servers to ensure scalability				
	- For the database architecture contractor can implement multiple instances of databases for required schemas or to use single instance with multiple schemas, but it must contain separate schemas for data preparation ("STG_" schema) , bad record data ("ERR_" schema), "live" data ("DWH_" schema) i.e. data to be used in BI system and "test live" data ("DWH_TEST_" schema) which will contain copy of live data for testing purposes				
	- Contractor is required to ensure existence of two parallel environments one for production and one for testing environment for all components of Business intelligence solutions (data warehouse, application server, business				

Item No	Specifications	Qty	Specifications Offered	Notes, remarks, ref to documentation	Evaluation Committee's notes

	intelligence, etc.)
	
	- Test BI environment also must be implement for testing, development and training which will be same as the production environment but limited to 10 test users
	
	- Implemented solution must include following data marts :
	
	  o COURT CASES with all information related to court cases but not limited to documents, state, information on institution, judge, etc.,
	
	  o PROSECUTION CASES with all information related to prosecutorial cases but not limited to documents, state, information on institution, prosecutors, etc.,
	
	  o HRMIS DATA with all information related to appointed carriers of judicial functions but not limited to documents, exam results, information on institution, number of case per judge/prosecutor, etc. and possible deviations/ abbreviation/ combination of listed data marts
	
	- Contractor is required to implement of "near-live" data quality system with following characteristics:
	
	  o "Near-live" data quality system need to be implemented on production data which is located on standby database				

Item No	Specifications	Qty	Specifications Offered	Notes, remarks, ref to documentation	Evaluation Committee's notes
	o Data quality system must include the records which failed the data validation/verification in the ETL procedures for data warehouse				
	o Data quality system need to be easily managed thru dedicated interface				
	o Data quality system must be able to run at specified intervals and to generate data quality reports				
	o Data quality reports must be delivered to users responsible for the quality of the data in respective institution				
	o Data quality system need to have detail log on when data error was recorder and when the report was sent and when the data was corrected				
	o Users designated for the data quality after receiving alert the data error was recorded must be able to access application/web portal to review data that has errors i.e. data which failed the data quality check				
	- Contractor is obligated to create 5 interactive portals/pages/dashboards for managerial purposes which will be used as tool for improving managerial capabilities. These 5 interactive portals/pages/dashboards (Managerial Overview - summary information from all other pages, Case flow, Realization of individual norms, Case plan realization,				

Item No	Specifications	Qty	Specifications Offered	Notes, remarks, ref to documentation	Evaluation Committee's notes

	Realization of foreseeable timeframes, Overview of solved and unsolved cases) will contain reports and graphs representing respective data
	
	 - Contractor will enable integration of BI components (reports, graphs, alerts, etc.) into existing judicial web portal
	
	    o Implemented BI solution must integrate into existing web portal to present the data in forms of graphs or reports on specified location on web portal (web portal is based on ADF technology running on Oracle IAS 10g server
	
	    o Certain group of reports needs to be presented on the restricted part of the judicial web portal. It would be good solution if the reports can just be changed in the BI and the updated reports presented on the web portal
	
	 - Contractor will provide 5 days training at HJPC premises for read-write users and administrator users for creating/editing/publishing of BI content
	
	 - Contractor will provide 2 days training for administrator at HJPC premises for administration of the BI solution
	
	 - create project, system and user documentation in electronic form available for on-line (web) presentation on the official languages of Bosnia and Herzegovina
	
	 - The contractor is required to install all necessary software,				

Item No	Specifications	Qty	Specifications Offered	Notes, remarks, ref to documentation	Evaluation Committee's notes
	configure date warehouse ETL procedure, establish data warehouse , implement BI, prepare required data marts, configure required interactive panels/pages/dashboards, conduct testing, training, deliver documentation in period of 10 months (305 days) from date of contract signing				

Delivery location:

Institution	Address
High Judicial and Prosecutorial Council of Bosnia and Herzegovina	**Kraljice Jelene 88, Sarajevo**

LOT 2 - Comprehensive Data Loss Prevention Solution

The purpose of this LOT is procurement of **Comprehensive Data Loss Prevention Solution** including the delivery of software (and hardware, as required), perpetual licenses, 1 year official manufacturer's software maintenance for the offered solution and all its components/modules/sub-systems, implementation services, consulting services and education services.

The solution shall significantly increase the security of classified, confidential and sensitive data at High Judicial and Prosecutorial Council of Bosnia and Herzegovina (HJPC) as well as courts and prosecutors' offices in Bosnia and Herzegovina. The primary goals of the solution are to:

- Identify, monitor, and protect confidential data at rest, in motion, and in use through deep content analysis based on centrally defined policies
- Make sure confidential data does not leave the organization inappropriately
- Automatically enforce data loss policies
- Secure data when it's stored on desktops, laptops, removable media, tablets, smartphones and other mobile devices
- Prove compliance with advanced reporting and auditing capabilities; monitor real-time events and generate detailed reports
- Enable comprehensive and effective classification of messages, documents and all other types of files and trigger additional levels of protection based on the classification; support automatic and user-driven classification.
- Enable enforcement of data leakage / loss prevention policies and measures to designated mobile devices and allow for its centralised management and overview

Abbreviations: DLP – Data Loss Prevention;

Subject of this procurement is the **Comprehensive Data Loss Prevention Solution** (encompassing the necessary software and hardware components/modules/sub-systems for execution of the required DLP functions), perpetual licenses, 1 year official manufacturer's software maintenance for all offered software, implementation services, consulting services and education services. Item numbers correspond to the following Table containing Specifications Required. The solution has to be industry well accepted with proven track record and with market presence at least as of mid-2013.

Explanatory note: Proposed solution has to include all necessary hardware for optimum functioning of the proposed DLP solution, if applicable. In practice, solution can be implemented through dedicated hardware or virtual appliances. In case of use of the virtual appliances, appropriate hardware for its optimum functioning needs to be provided, taking in consideration up-scaling of the system to include at minimum 5500 clients.

Physical components have to be delivered to designated locations.

All third party software licences needed for the implementation of the required solution must to be included in the proposal.

1. COMPREHENSIVE DLP SOLUTION

System should be designed to detect potential data leakage and prevent them by monitoring, detecting and blocking sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage).

Judicial Communication Network includes around 100 physical locations which need to be covered by the proposed DLP Solution. Data Centre is located at the premises of the High Judicial and Prosecutorial Council BiH (Sarajevo). DLP Solution needs to be implemented at the HJPC's Data Centres. All judicial institutions (users) have the access to the HJPC Data Centre through the links of varying data transfer capacity. Regional centres situated in Banja Luka, Tuzla and Mostar have the access to the HJPC DC through the link with speed/capacity 100 Mbps. As well as the HJPC DC, these centres represent the aggregation points. Judicial institutions from other locations situated outside these three locations access these regional centres through links of average capacity of 4 Mbps. These links are used to enable user access to all Judicial Information System's services including Case Management System, e-mail, internet access, etc. It is crucial to ensure the optimisation of the DLP solution not to affect optimum functioning of all the existing services.

The solution will include the following functions:

1.1. DLP MANAGEMENT and REPORTING

Solution will allow centralized and intuitive management, administration and out-of box patching for all of the parts of the Comprehensive DLP Solution. It shall also provide advanced reporting functionalities.

1.2. DLP POLICIES MANAGEMENT

Solution should have centralized web-based interface for all aspects of policy editing and policy management, across all products and predefined detection policies to cover regulations and detection best practices.

1.3. DLP DISCOVERY and CLASSIFICATION

Discovery, detection and classification of confidential data at storage locations, databases, including encrypted repositories (including ability to decrypt for purpose of policy matching) and apply security policies to large quantities of any type of documents (including, but not limited to MS Office, e-mail messages, generic files of any sort).

1.4. NETWORK DLP

Monitor, analyse and conditionally prevent web, e-mail and other network traffic. Solution to be used for monitoring and capturing all network traffic at the critical network nodes which is protocol agnostic and can capture and index all network traffic, conduct forensic analysis to correlate current and past risk events, detect risk trends, and identify threats.

1.5. ENDPOINT DLP

Solution needs to have the ability to detect and prevent loss and leakage of data from the end-user side. Solution will also enable encrypting drives, files, folders and removable media and remote management

2. MOBILE DLP

Solution needs to provide data loss prevention function for mobile devices (smartphones).

3. Implementation services, consulting services and education services for COMPREHENSIVE DLP SOLUTION and MOBILE DLP (Items 1 and 2)

Required implementation services, consulting services and education services are specified in the below Table containing Specifications Required.

Item Number	Specifications Required	Qty	Specifications Offered	Notes, remarks, ref to documentation	Evaluation Committee's notes
1	**COMPREHENSIVE DLP SOLUTION** **Licenses required:** Perpetual licenses for 2000 nodes / clients **Official manufacturers maintenance required:** 1 year from the date of Provisional Acceptance **Miscellaneous:** Solution needs to encompass the necessary software and hardware components/ modules/ sub-systems for execution of the required DLP functions (1.1 – 1.5). The solution must be available in a stand-alone form and should not be based on offerings embedded within other suites or products. **Platform characteristics and general requirements:** - Integration with Active Directory (Windows server 2012, authentication and authorisation enabled through AD services), - Compatibility with Windows File Security Services (including NTFS), - Integrate with ICAP-enabled web proxies (including BlueCoat), - Integrate with any SMTP-compliant MTA (including Symantec SGS), - Integration with Microsoft Exchange 2010.	2000			

Item Number	Specifications Required	Qty	Specifications Offered	Notes, remarks, ref to documentation	Evaluation Committee's notes
	The solution will include the following functions:				
1.1	**DLP MANAGEMENT and REPORTING** System should use a single unified console for all configuration and reporting operations across all detection paths, storing all captured data and logs in a centralized database, thus providing centralised and intuitive management, administration and out-of-box patching. The system should have the ability to scale to protect tens of thousands of agents. System should have: - Automated software updates from centralized console to servers and endpoints, - Enterprise-class database for high scalability, high performance and clustering support, - Encryption mechanisms in full compliance with PCI data handling standards, - Data stored in incident database in encrypted format - Detailed activity audit logs of database transactions and policy modifications, - Fully customizable response interface allowing combinations of multiple remediation actions in a single UI action, - All relevant incident details on a single page to allow quick user decision-making and action.				

Item Number	Specifications Required	Qty	Specifications Offered	Notes, remarks, ref to documentation	Evaluation Committee's notes
	System should have the ability to: - Store multiple years of incident data in a centralized database - View full incident history including all changes and edits to that incident, - Define custom incident attributes (e.g., department, business unit, sender contact information, incident cause, etc.) and populate either automatically from directory lookups or manually. System should provide: - Custom report filtering across different variables and attributes, - Reports that summarize incidents and incident trends by department or by organization - Insight into the behaviour of specific individuals and focus on those users posing the highest risk System should have: - Single user interface for all incidents (storage, network, and endpoint) as well as for systems management - Configurable risk dashboards simultaneously showing different reports from storage, network, and endpoint System should have the ability to: - Send any report via email, either on command or via				

Item Number	Specifications Required	Qty	Specifications Offered	Notes, remarks, ref to documentation	Evaluation Committee's notes
	regularly defined schedule - Run reports on large incident databases with minimal performance impact				
1.2	**DLP POLICIES MANAGEMENT** System should have centralized web-based interface for all aspects of policy editing and policy management, across all products and predefined detection policies to cover regulations and detection best practices. System should have the ability to: - Define policies based on any of the following: content, sender/recipient, file characteristics, communications protocol, endpoint user, and endpoint location, - Integrate directly with Active Directory to create user- or group-based detection rules, - Export and import policy templates,				
1.3	**DLP DISCOVERY and CLASSIFICATION** Solution needs to provide discovery and detection of confidential data at storage locations, databases, including encrypted repositories (including ability to decrypt for purpose of policy matching) and apply security policies to large quantities of any type of documents (including, but not limited to MS Office, e-mail messages, generic files of any sort). Solution will enable comprehensive and effective				

Item Number	Specifications Required	Qty	Specifications Offered	Notes, remarks, ref to documentation	Evaluation Committee's notes
	classification of structured and unstructured data (messages, documents and all other types of files) and trigger additional levels of protection based on the classification. The solution will support automatic (policy based) and user-driven file classification (if the user-classification tool is not an integral part of the solution, appropriate classification tool(s) need to be included in offer).

System should also have the ability to:
- Detect both structured (SSNs, CCNs, etc) and unstructured classified data (MS Office docs, PDFs, CAD/CAM diagrams, source code, etc),

- Detect large volumes of structured and unstructured classified data

- Extract and inspect the text content of files and attachments,
- Automatically notify senders or their managers when a policy has been violated,
- Configure multiple automated responses based on severity, match count, policy, etc.
System should have:
- Option to permit any or all data owners to send their own personal data (such as their own personal credit card | | | | |

Item Number	Specifications Required	Qty	Specifications Offered	Notes, remarks, ref to documentation	Evaluation Committee's notes
	number) outside the corporate network without violating a classified data detection rule, - Pre-built ability to detect a wide range of data patterns that represent confidential data (e.g., CCNs, BINs, magnetic stripe data, IBAN), - Detect sensitive content using at least three of the following content-aware detection techniques: partial and exact document matching, structured data fingerprinting, statistical analysis, extended regular expression matching, and conceptual and lexicon analysis - Enable applying visual labels and markings to documents in accordance with document classification. System should also have the capability to: - Scan Microsoft .pst files with the ability to identify confidential data on a per message basis, - Scan encrypted repositories with the ability to decrypt and evaluate for policy matching, - Scan Oracle, SQL, DB2, Sybase, SharePoint, Exchange and web sites, - Scan Windows file systems via CIFS, - Scan Unix file systems via NFS, - Scan local Windows file systems, - Scan local UNIX file systems (Linux, AIX, and Solaris), - Automatically copy (tag), relocate (quarantine) or apply digital rights (Microsoft RMS) to discovered confidential				

Item Number	Specifications Required	Qty	Specifications Offered	Notes, remarks, ref to documentation	Evaluation Committee's notes
	files which violate policy, - Configure and control all scanning from a single, centralized console, - Scan systems at remote locations with limited network bandwidth. The solution should not: - Use only simple data detection mechanisms (e.g. keyword matching), - Primarily support DLP policy enforcement via content tags assigned to objects.				
1.4	**NETWORK DLP** Solution needs to be able to monitor, analyse and conditionally prevent web, e-mail and other network traffic, including monitoring and capturing all network traffic at the critical network nodes which is protocol agnostic and can capture and index all network traffic, conduct forensic analysis to correlate current and past risk events, detect risk trends, and identify threats. System should have the ability to: - Analyze traffic and report incidents in real-time. Monitor email traffic, including attachments, without adding latency or failure points to the network, - Monitor web traffic, including web mail, web postings, and other protocols using HTTP (including uploaded files),				

Item Number	Specifications Required	Qty	Specifications Offered	Notes, remarks, ref to documentation	Evaluation Committee's notes
	- Block and quarantine emails that are in violation of company policy on confidential data, - Receive notification of a blocked or quarantined email, - Monitor corporate email and web accessed from smartphones and tablets, - Filter out network traffic for inspection based on protocol, IP range, or email sender/recipient email - Provide detailed traffic statistics for overall data throughput, number of messages, and number of incidents on a per protocol basis - Conditionally block HTTP, FTP, SMTP, and encrypted web transmissions based on message content - Integrate with any SMTP-compliant MTA - Integrate with ICAP-enabled web proxies (including BlueCoat), - Supports network prevention products running in a VMware image				
1.5	**ENDPOINT DLP** Solution needs to have the ability to detect and prevent loss and leakage of data from the end-user side. Solution will also enable encrypting drives, files, folders and removable media and remote management. If encryption tool is not an integral part of the solution, appropriate encryption tool(s) need to be included in offer.				

Item Number	Specifications Required	Qty	Specifications Offered	Notes, remarks, ref to documentation	Evaluation Committee's notes
	System should have the ability to detect user attempts to: - Copy confidential data to removable storage devices (USB drives, CD/DVD, SD/CF cards, etc.), - Download confidential data (in structured and unstructured format) to their hard-drives, - Print, copy, or paste confidential information. System should also have the ability to: - Automatically encrypt confidential data upon copy to USB - Monitor/block HTTP, HTTPS, IM, FTP transmissions, - Monitor/block data copied to or from network file shares via Windows Explorer, - Block print screen actions, - Encrypt and authenticate communications between agent and server, - Support global distributed deployments of endpoint machines, - On-screen, pop-up notification with fields for user justification can appear upon the generation of an incident, - Endpoint user self-remediation (on-screen notification prompting user to confirm whether to continue or cancel confidential data transfer)				

Item Number	Specifications Required	Qty	Specifications Offered	Notes, remarks, ref to documentation	Evaluation Committee's notes
	- Provide continuous protection of confidential data regardless of whether the user is on or off the network - support latest OS (including Windows 8.1).				
2	**MOBILE DLP** Solution needs to provide data loss prevention function for mobile devices (smartphones). **Licenses required:** Perpetual licenses for 200 devices **Official manufacturers maintenance required:** 1 year from the date of provisional acceptance **Miscellaneous:** Installed software must include appropriate number of licenses. **Minimum functional and technical requirements:** - Offered solution needs to feature DLP at the level of mobile device, applications and data, - It should enable an integrated approach to managing data security on mobile devices, - support for major smartphone platforms - Enable centralised policy configuration and management and reporting - Enable policy enforcement on mobile devices - Assure mobile security environment for running of business applications (primarily e-mail exchange)	**200 licences**			

Item Number	Specifications Required	Qty	Specifications Offered	Notes, remarks, ref to documentation	Evaluation Committee's notes

3	**Implementation services, consulting services and education services for ITEMS 1 and 2** (encompassing all prescribed functions)
	
	Minimum required amount of professional services delivered by experienced, trained and certified professionals must include:
	- Preparation, Pre-Engagement, Assessment and Planning
	  o Conduct Data Governance and Element Definition Workshop(s)
	  o Produce a solution architecture overview
	  o Review architecture, email, networking, and application teams
	- Design
	  o Define configuration and integration parameters
	  o Development of device definitions, device rules, classification rules, removable storage protection rules, email protection rules, web post protection rules
	- Implementation, integration and training
	  o Install and configure the solution
	  o Fully integrate all solution components
	  o Integrate solution components with central management console
	  o Setup of directory services (LDAP/AD) integration
		1			

Item Number	Specifications Required	Qty	Specifications Offered	Notes, remarks, ref to documentation	Evaluation Committee's notes
	o Develop scheduled reports o Develop scanning schedules and targets o Develop capture filters o Activate appropriate prebuilt policies/rules o Configure discover scans o Configure device policies o Configure load balancing and network optimization o Development and customization of templates, concepts, rules, policies and action rules o Deploy the DLP policies to appropriate deployment targets o Configure required groups and users o Develop filters, rules, policies, and templates o Implement device definitions, device rules, classification rules, storage protection rules, email protection rules, web post protection rules o Activate appropriate policies/rules o Tune rules and modify responses o Provide Solution user acceptance test for the complete solution o Provide a Go-Live procedure and Initial support o Provide training for 6 (six) IT administrators and staff that should include "on site" training for administrators and to engage them during the				

Item Number	Specifications Required	Qty	Specifications Offered	Notes, remarks, ref to documentation	Evaluation Committee's notes
	whole system installation and configuration process (Training must include knowledge transfer for the installation, configuration, and administration of the solution.) The maximum duration of the above listed services is **210 working days**, with the following indicative schedule: - Installation of DLP in test environment and adjustment of DLP system, configuration and fine-tuning of policies, including training of ICT personnel – **120** working days - Installation of DLP system in production environment and pilot implementation in chosen judicial institutions and training – **90** working days				
	ANCILLARY SERVICES for LOT 2: - The Contractor needs to deliver all specified equipment and on-the-shelf software, install, configure and integrate all new components with the existing HJPC's infrastructure, test and made operational the whole system. - The Contractor needs to document the implemented system through system, user and technical documents. All documentation should be available in digital format and written in one of the official languages used in Bosnia and Herzegovina. Original technical documentation can be written in English.				

Delivery location:

Institution	Address
High Judicial and Prosecutorial Council of Bosnia and Herzegovina	**Kraljice Jelene 88, Sarajevo**