ANNEX II + III: **TECHNICAL SPECIFICATIONS + TECHNICAL OFFER**

Contract title: Common Information System for Vetting and Issuing of Security Clearances

Publication reference: EuropeAid/140099/DH/SUP/BA

Tender Number: EC/BiH/TEN/16/020

Columns 1-2 should be completed by the Contracting Authority
Columns 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.

1. Item Number	2. Specifications Required	3. Specifications Offered	4. Notes, remarks, ref to documentation	5. Evaluation Committee's notes
Delivering and configuring hardware and integrated software development to establish a unique security vetting and security clearance management system (SCM). The system will be established between four institutions, namely the Ministry of Security of BiH (MoS), the Ministry of Defence of BiH (MoD), the Intelligence and Security Agency (OSA) and the State Investigation and Protection Agency (SIPA). The Central Registry and the central location of the system with the servers will be located at the MoS premises in the Parliament building (Trg BiH 3). Clients to be connected are located in the MoD, the OSA, the SIPA and partly also in the dependence of the MoS in the Council of Ministers building (Trg BiH 1). **Warranty requested:** • Warranty period for all items: 1 year • Commercial warranty as granted by the manufacturer				
1.1	**Cabling – 350 meters – Connection between two locations of the MoS** **(one location is in Parliament building-1st floor, second one is located in Council of Ministers building-13th floor)** a) Cable: Fibre-optical, Multimode, 8 fibers, min. 350 meters b) Protection: halogen-free outer jacket c) Patch panel: (2 packages – for each end), Fibre-optical; d) Equipped with: Splice box; 8 x SC pigtails 2m (with ceramic ferrule, slide mechanism; 8 x SC connector pre-installed on patch panel (4 x blank cover included for unused ports) e) Installation: in-building mounting and connecting (splicing) cable to patch panels on both ends; patch panels installation into existing communication cabinets			

1. Item Number	2. Specifications Required	3. Specifications Offered	4. Notes, remarks, ref to documentation	5. Evaluation Committee's notes
1.2	**Barcode Label printer – 5 pcs** a) Print method: direct thermal b) Connectivity: USB, Ethernet c) Printer Specifications Resolution: 203 dpi/8 dots per mm d) Memory: min 4 MB Flash; min 8 MB SDRAM e) Print Width: 104-108 mm, f) Minimum Print Length: 300 mm (203 dpi), g) Minimum Print Speed: 100 mm per second (203 dpi), Delivery, installation and assembly and integration with other parts of the system, including delivery all necessary cables and connectors (Items number: 1.11, 1.17).			
1.3	**Laser Barcode Scanner - 30 pcs** a) Scanner Type: Bi-directional b) Light Immunity: min 75,000 Lux c) Light Source (Laser): visible 650nm laser diode (+/- 10 nm) d) Scan speed: min 100 scans per second e) Interfaces Supported: USB, RS-232; Keyboard Wedge f) Beeper Tone: Beeper (adjustable tone) Delivery, installation and assembly and integration with other parts of the system, including delivery all necessary cables and connectors (Items number: 1.11, 1.17).			

1. Item Number	2. Specifications Required	3. Specifications Offered	4. Notes, remarks, ref to documentation	5. Evaluation Committee's notes
1.4	**Firewall type 1 – For central location - 2 pcs** a) Network interfaces: minimum 8 x 1Gbps (RJ45) b) RAM: 4GB minimum c) SSD: minimum 64GB d) Ports: 1x Console RJ 45, min 1x USB port e) Display: Integrated display on front device, f) Power: AC power supply, internal g) Rack mountable: 19" with rack mount kit h) Firewall throughput [Gbps]: minimum 3,8 Gbps, i) Concurrent sessions: minimum 375,000, j) New sessions/s: minimum 20,000 k) VPN throughput: minimum 300 Mbps, l) IPS throughput: minimum 250 Mbps, m) Filter: Mail Gateway & Spam Filter, Web Filter n) Control: Application Control and granular application enforcement o) Security: Interception and decryption of SSL/TLS encrypted applications, IDS/IPS, Protection against exploits, threats and vulnerabilities Delivery, installation and assembly and integration with other parts of the system, including delivery all necessary cables and connectors (items number: 1.1, 1.5, 1.6, 1.12, 1.14, 1.17)			

1.5	**Firewall type 2 – For remote locations - 3 pcs** a) Connectivity: Network interfaces: minimum 4 x 1 Gbps (RJ45) b) RAM: minimum 4 GB, Storage mass: SSD, minimum 8GB c) 1x Console RJ 45, min 1x USB 2.0 port d) Desktop, wall mount (wall mount bracket included) e) AC power supply external or internal f) Firewall throughput [Gbps]: minimum 1 Gbps g) Concurrent sessions: minimum 64,000 h) New sessions/s: minimum 5,000 i) IPsec VPN throughput: minimum 200 Mbps j) IPS throughput: minimum 150 Mbps k) Application Control and granular application enforcement l) Interception and decryption of SSL/TLS encrypted applications, IDS/IPS m) Protection against exploits, threats and vulnerabilities n) Advanced anti-evasion and obfuscation techniques o) DoS/ DdoS, ARP spoofing p) DNS reputation filtering Delivery, installation and assembly and integration with other parts of the system, including delivery all necessary cables and connectors (Items number: 1.4, 1.11, 1.17).			

1.6	**Network switch for the Central location – 2 pcs** a) DRAM: minimum 1 GB b) Flash: minimum 1 GB c) Connectivity: Network interfaces min 24 x 1Gbps (RJ45); min 4-port uplinks (GbE (SFP) or 10GbE (SFP+) – with included appropriate modules) d) 1 x Serial; 1 x 10/100/1000Base-T management port e) Packet Switching Capacities: min 88 Gbps f) Rack mountable: 19" with rack mount kit g) Power supply: AC power supply h) Routing: Supported Layer 2 and Layer3 i) Management: Web interface for configuration j) MAC table size: minimum 16,000 entries Delivery, installation and assembly and integration with other parts of the system, including delivery all necessary cables and connectors (Items number: 1.4, 1.7, 1.9, 1.11, 1.14, 1.17).			
1.7	**Servers Type 1 – For Central location, 2 pcs** a) Rack mountable: 19" 1U or 2U; rack, with all the necessary options for installation in the rack b) Processor: minimum Pass mark CPU Mark 23000 (min 24.75 MB cache); installed two processors with minimum 12 cores per processor c) Memory: min 256 GB DDR4 SDRAM ECC - expandable to 1.5 TB - with LRDIMM / RDIMM modules; d) Network interfaces: Integrated minimum 4 x Gigabit Ethernet (10/100/1000) and Dual Port 16Gb Fibre Channel HBA e) Power supply: dual and redundant, at least 2 x 550W AC; Optical drive: External or Internal Multi-burner			

	optical f) Controller: SAS / SATA controller supports RAID 0, 1, 1 + 0, 5; g) Installed RAID 5; h) HDD: Built-in minimum 3 x minimum 300GB 10K 12Gbps SAS (RAID5); expandable to a minimum of 24 Hot Swap HDD and the possibility of combining SATA, SAS and SSD drives simultaneously i) Front ports: minimum 1 x USB 3.0 ports; 1xVideo Failure detection: The detection of defects in the system: CPU, memory, VRM, disks, power supplies and fans: j) Virtualization: Installation and configuration of 2 virtual machines in total. k) Operating system: Installation and configuration of operating system on virtual machines (Two licenses of Microsoft Windows Server Standard will be provided by the beneficiary). Configuration to operate with overall system. Configure Failover Cluster feature with 2 nodes (2 servers). l) Database system: Installation and configuration of Microsoft SQL Server Standard with the integration with the overall system. (License provided by the beneficiary) – integration and configuration with items number 1.14 and 1.18 Delivery, installation and assembly and integration with other parts of the system, including delivery all necessary cables and connectors (Items number: 1.4, 1.5, 1.6, 1.8.(second server) 1.9, 1.10, 1.11, 1.12, 1.13, 1.14, 1.16, 1.17).			

1.8	**Servers Type 2 – for Central location and for SIPA - 2 pcs** a) Rack mountable: 19" 1U or 2U; rack, with all the necessary options for installation in the rack b) Processor: minimum Pass mark CPU Mark 10800; installed two processors with minimum 4 cores per processor c) Memory: min 128 GB DDR4 SDRAM ECC - expandable to 1.5 TB - with LRDIMM / RDIMM modules, min 24 dimm. slots; d) Network interfaces: Integrated minimum 4 x Gigabit Ethernet, extra Quad Port GbE Adapter (total 8x10/100/1000) and Dual Port 16Gb Fibre Channel HBA e) Power supply: dual and redundant, at least 2 x 550W AC; f) Optical drive: External or Internal Multi-burner optical drive (optional), g) Controller: SAS / SATA controller supports RAID 0, 1, 1 + 0, 5; h) HDD: Built-in minimum 5 x minimum 600GB 10K 12Gbps SAS (1GB Flash/RAID 5); expandable to a minimum of 24 Hot Swap HDD and the possibility of combining SATA, SAS and SSD drives simultaneously i) Front ports: minimum 3 x USB ports; The detection of defects in the system: CPU, memory, VRM, disks, power supplies and fans **First server**: Operating system: Installing only the operating system (License of Microsoft Windows Server Standard will be provided by the beneficiary). Installation and configuration of Active Directory-Domain Name System and migration from the existing AD-DNS. Integration with overall system. **Second server:** Operating system: Installing the operating system (License of Microsoft Windows Server Standard will be provided by the beneficiary).			

1.9	**SAN switch - 1 pcs** a) Form factor: 1U rack mount b) Ports: 48 SFP/SFP+ ports. Minimum 12 ports licensed by default; additional minimum 12-port license pack c) Media types: minimum 8 Gb FC and 16 Gb SFP+ transceivers d) FC Speed Support: 16/8/4/2Gbps e) Transceivers: Set of 24 Pcs SFP+ 16Gb FC transceivers f) Power supply: redundant hot-swap, g) Hot-swap parts: SFP/SFP+ transceivers, power supplies with fans, h) Management ports: One 10/100 Mb Ethernet port (UTP, RJ-45); one RS-232 port (RJ-45); one USB port i) Secure Socket Layer (SSL); IP security (IPsec) j) Cords: Set of Fibre Patch Cords (LC – LC) Cables - Compatible for connecting storage (1.10) and HBA Cards on the servers (1.7) Delivery, installation and assembly and integration with other parts of the system, including delivery all necessary cables and connectors (Items number: 1.7, 1.10, 1.12, 1.14, 1.17).			
1.10	**Storage - 1 pcs** a) Supported connections to servers: min 6Gb SAS, 8Gb FC b) Installed connection to servers: 8×16Gb FC ports (4 ports per controller) include all SFP modules c) Processors: Min 1×quad-core Processor or 2×two-core processor d) Web-based GUI e) Controller: Dual and redundant f) Cache: min. 16 GB g) Type of discs: Dual-port, hot-swappable 12GB SAS drives h) Supported number of discs: a minimum of 240 SFF drives i) Supported mixing different types of drives: SAS, SSD			

	j) Installed drives: minimum 6x800GB 2.5-inch Flash Drive and 18x1.2TB 2.5-inch 10K HDD k) RAID levels: RAID 0, 1, 5, 6 and 10 l) Fans and power supplies: Hot-swap, full redundancy m) Rack format: standard 19", rack, with all the necessary options for installation in the rack n) Cables: All Cables necessary to connect to other components of the system and power cables included Delivery, installation and assembly and integration with other parts of the system, including delivery all necessary cables and connectors (Items number: 1.7, 1.9, 1.12, 1.14, 1.16, 1.17).			
1.11	**Desktops - 30 pcs** a) Processor: min. dual core, min. Pass mark CPU Mark score 7800 or higher b) Memory: minimum 4GB DDR4 2666MHz c) HDD: Minimum internal 500GB HDD SATA d) RAM expandable: to a minimum of 32GB; e) Optical drive: DVD RW drive, f) Ethernet: Integrated Gigabit Ethernet (10/100/1000) g) Graphics: Integrated graphics; h) Accessories front: minimum 2 x USB ports, a microphone input and headphone; i) Accessories back: minimum 4 USB ports, VGA + (HDMI or DVI), Serial port integrated j) Monitor: display size min. 21.5'' Full HD LED, the response of max. 5 ms k) Keyboard: USB Keyboard - localized BiH language; l) Mouse: Optical mouse USB, 2 buttons (with scroll); m) Operating system: Preinstalled Operating System. Has to support integration with overall system. Delivery, installation and assembly and integration with other parts of the system, including all necessary cables and connectors: (Items number: 1.5, 1.6, 1.7, 1.8, 1.10, 1.13, 1.15, 1.17).			

1.12	**UPS – 2 pcs** a) Form Factor: rack-mountable b) VA/Watts rating: min 5000 VA/4500 W c) Input/ Output Voltages: 230V d) Full load autonomy: minimum 20 minutes e) Frequency Required: 50/60 Hz f) Output Connector Type: power IEC 320 C13 g) Output power Connector: min qty 6 h) Battery type: leak-proof i) Communications and management: USB port (Type B), RS-232 serial port (RJ-45), LCD display, LED indicators Delivery, installation and assembly and integration with other parts of the system, including delivery all necessary cables and connectors (Items number: 1.4, 1.6, 1.7, 1.9, 1.10, 1.14).			
1.13	**Fast document scanner – 5 pcs** a) Type: Automatic Document Feeder (ADF) scanner b) Resolution: Scanning resolution: min. 600 dpi c) Type of scan: Monochrome, Grayscale & Colour d) Scanning speed: Monochrome: min 120 image/min - Colour: min 120 image/min measured with size: A4, resolution: 200 / 300 dpi, duplex, e) Scanning Side: Front/ Back/ Duplex f) Document Feeding: Automatic document feeder (ADF) min 80 sheets g) Interface: min USB 2.0 Delivery, installation and assembly and integration with other parts of the system, including delivery all necessary cables and connectors (Items number: 1.11, 1.17).			

1.14	**Server Rack Cabinet – 1 pcs** a) Description: 42U Rack metal cabinet b) Material: metal with antistatic coating c) Rack Height: 42U d) Panels: Lockable doors and side panels e) Optimization: Thermal optimization f) Doors and wheels: Doors and mobility doors that can be locked, all sites must be detachable, Rack must be on wheels and easy to move. A split rear door for easy access for serviceability; Outriggers with wheels for stability during loaded transport; A perforated front door g) Cables: Rear cable management channels with space for mounting 0U strip PDUs h) KVM: Rack mountable KVM switch Console 1x8 with 8 x cables, with rack mountable kit i) PDU: Sidewall compartments (pockets) for 1U PDUs j) Installed: 2×50A PDU with minimum 12 sockets (European 220-230V) k) Console: 1U flat panel monitor console kit with Keyboard tray including minimum display size 17'' LCD/LED monitor and keyboard with localized BiH keyboard l) Possibility of installation in the rack: Servers, Storage, a UPS and other equipment offered, 19 "industry-standard, Delivery, installation and assembly and integration with other parts of the system, including delivery all necessary cables and connectors (Items number: 1.4, 1.6, 1.7, 1.9, 1.10, 1.12).			

1.15	**Laser Printer – 5 pcs** a) Type: Colour b) Technology: Laser printer c) Speed Colour: up to 31ppm Colour Print d) Speed Monochrome: Up to 38ppm Mono Print e) First Page: max 12 Seconds First page f) Double Sided Printing: Automatic Double Sided Printing g) Maximum Paper Size: A4 h) Printer Resolution: min 600 x 600 dpi Print i) Interface Type(s): USB & Network j) Processor: min 500MHz k) Memory: min 1GB RAM l) Paper Handling Input 1: min 250 Sheet Input Tray m) Paper Handling Input 2: min 100 Sheet Multipurpose Tray n) Paper Handling Standard Output: min 150 Sheets o) Sheet Weight: 60 to 210g/Sq m p) Emulations: min PCL5/6 & Postscript 3 Delivery, installation and assembly and integration with other parts of the system, including delivery all necessary cables and connectors (Items number: 1.11, 1.17).			
1.16	**Virtualization Software-1 pcs** a) Licenses: Software for servers virtualization (licenses for 4CPU-2 servers with 2 CPU) b) Features includes: 1. Proposed solution must support virtualization based on x86 platform. 2. Proposed solution must provide ability to over-provision virtual memory, 'Dynamic Memory'. 3. support live migration without VM downtime 4. possibility to restart the virtual machine on a second physical server in case of failure of the virtual machine on the first physical server, or the first physical server itself. 5. Proposed solution must provide ability to			

	perform concurrent live migrations on a single host to reduce time it takes to evacuate all VMs on a single host during planned maintenance. 6. Proposed solution must have a support for a broad set of Windows guest server & client OSs back to Windows 2000. Support for all major Linux distributions, including para-virtualized Linux. 7. ability to take snapshots of live running VMs and restore to a snapshot point without powering down the VM 8. Proposed solution must provide support for centralized management of virtual machines and hosts from one location. Solution must support utilization monitoring of virtual machines and hosts. 9. Installation: Full installation and configuration of the virtualization software (min. two hosts virtual servers) including testing, installation, configuration and integration. Delivery, installation and assembly and integration with other parts of the system (Items number: 1.7, 1.9, 1.10).			
1.17	**Software, database and reports development, installation, configuration, integration as well as induction training for Administrators and Users** **1. Architectural Goals and Constraints** The overall architecture goal of the system is to provide a highly available and scalable web-services exchange service for “need to know” users employed by agencies. Web-services exchange service has to enable users to understand what services are available for use.			

	a) Security Requirements SCM should implement secure storage of SCCs (Security Clearance Certificates) and secure intra-agency communication, all the associated safety operating procedures, protection from a large number of threats such as unauthorized access to the network, loss of confidential information, information system breaches, leak of classified documents, and others. Implementation of security management system should aim to ensure the security of information resources in three main aspects: confidentiality, integrity and availability. SCM should be in full compliance with NATO and EU security guidelines and directives, and also with regulations issued by relevant authorities in B&H. SCC term encompasses both Personal Security Clearance (PSC) and Facility Security Clearance (FSC). **b) Standards-Based** The standards-compliance will not only apply to service functionality but also to design, platform/infrastructure and other parts of the Security Clearance Management (SCM) system. Examples of standards include HTTPS, XML, SOAP and WSDL. **c) Collaboration Enabling** The system should be a multi-user distributed system that allows the authorized users to interact in the creation/modification of a document. Document owners can see all accesses and modifications as they occur. **d) Portability** Portability should be supported as follows: • Data Structures Adaptability: The database and files used by the SCM systems should be able to easily be transferred to another computer station without any loss regarding data integrity. This must be achieved without any changes to users' systems.			

	• Hardware Environment Adaptability: The SCM systems must have the ability to be transferred to alternative computer equipment platforms, either locally or in a completely different place, without data loss and without any changes to users' systems. • Organizational Environment Adaptability: The SCM systems must be able to be transferred to alternative computer equipment platforms without code changes and changes to any systems that interface with it. • Available Coexistence: The SCM systems must be able to coexist on the same computer equipment. **e) Usability** A system is considered friendly if the following requirements are met: • Products and documentation: Although the system is better to be used without the use of devices, however, the existence of such devices is necessary. Support mechanisms should be available to assist the user (e.g. on-line help, hints and tips, dictionary help, context-sensitive help, etc.). • Recover from error: In case of operating fault, a controlled screen and a message should be presented in the user's screen for the next steps. Any work executed at that time by the user should not be missed. • Error Prevention: The design of the software application must be careful in order to prevent the presence of problems. There must be a limit of error cases or check for errors, which will be displayed on user's screens with a confirmation option before completing the transaction. The user should also have the ability to correct the error. • Ability to view the system status. The system should inform the users about what is happening with the appropriate feedback within a reasonable time. For example, the users should be alert in case of time-out before end of time.			

- Navigation. Users should be able to easily navigate throughout the system.
- Aesthetic and minimalist design. The user interface should be simple and uniform across all the application software processes.
- User Familiarity. The software application must be suitable for use by people with little knowledge in computers.

f) Distributed Workflow

Document information tracking objects are created by an authorized user and can subsequently be assigned to any authorized user. Further, authorized users can manage multiple document objects simultaneously without fear of confusion or productivity loss.

g) Real Time Progress Visibility

All document changes and modifications can be reviewed as they occur, security oversight teams can ensure that authorized users have done their due diligence relative to protection of sensitive information.

h) Security Oversight and Audit Reporting

The system would allow authorized users to print tracking lists, user rosters, activity reports. Any information entered during the course of its operation can be searched and retrieved for compilation into any type of report required for security handling procedure reviews or internal inspections.

i) Process Consistency

The system ensures that all document management procedures are performed in exactly the same way and that information deemed necessary is collected, entered and audited in accordance with government requirements.

2. Logical design

a) Locations

SCM system will be located at Server room at Central Registry (CR) for Security Clearance Certificates (SCC) at the building of the Parliamentary Assembly of Bosnia and Herzegovina (Trg Bosne i Hercegovine 1, Sarajevo).
Client workstations needed to access the service provided by SCM at the Central Registry will be located at the agencies premises. Server in SIPA (Nikole Tesle 59, Istočno Sarajevo) will serve internal application for security clearances within the competence of SIPA.
The communication will be provided through "B&H SDH" network maintained by IDDEEA (Agency for identification documents, registers and data exchange).

b) Capacity

Following numbers should be used as estimate although the system should be scalable to support larger number of users.
Number of Agencies: 15
Number of Users: 50
Number of concurrent requests: 10

c) Operation overview

Users from MoS and from remote agencies will be able to use SCM by means of workstation, and standard web browser GUI through the "B&H SDH" network.
Government Agencies which perform clearance review (background vetting) will be able to use either web browser GUI or XML data import/export functionality provided by SCM web browser GUI to exchange data with their current physically separated workflow software for the purposes of their internal data handling.

	3. Business Process Architecture **a) Required functionalities** Security Clearance Management (SCM) will as a minimum: **i. General requirements:** • Provide MoS with a centralized system for continued secure storage and life-cycle management of an issued Security Clearance Certificates (SCC) including PSC and FSC. • Provide secure and efficient intra-agency information exchange with regards to procedures and workflows related to SCC submission, issuing, validation and revocation. **ii. Workflow requirements:** • SCC **submission**: Provide entry point for candidate data and submit it for review (background vetting) to the designated Agency. • SCC **issuing and document generation**: Provide clearance background vetting validation. Upon final adjudication, the system would permit the issuing agency to print out an individual's clearance document. • SCC **validation**: Once a clearance has been issued, the SCM system will enable instant clearance validation to the agencies. This aspect is essential for ensuring that individuals with revoked or expired clearances do not gain access to sensitive or classified information. Further it prevents the passage of fraudulent credentials to gain access to sensitive information or areas. • SCC **revocation**: Provide authorization workflow for revoked clearances. • SCC **upgrade/downgrade**: Provide authorization workflow for upgrade or downgrade of classification level of existing clearances. • SCC **temporary authorization**: Provide authorization workflow for emergency temporary			

	clearances. • SCC **life-cycle management**: Provide automatic revocation of expired clearances or initiation of renewal. • Provide mechanism of vetting that **periodic security consultation** has been performed to refresh security awareness of individual clearance holder. • Enable **centralized clearance management**: Government Agencies and institutions will have an online (via secured network) capability to review candidate submissions, make adjudication decisions, review clearance holder histories and make annotations about possible security related incidents. This is envisioned to become the authoritative source by for the B&H government to make information available to any group or office requiring it. • Enable **distributed background vetting**: the agencies performing background vetting will have an online (via secured network) capability to receive requests, make annotations and deliver their reports. Enable **creating of statistical reports and diagrams** regarding issued Security Clearance Certificates (PSC and FSC) (i.e. number of issued certificates for some period with their security level and their owners, number of rejected requests etc.) **iii. Data migration** Data migration from existing database, stored in Microsoft SQL Server 2014, into new system. **b) Architectural requirements** • **Collaboration and distributed workflow**: SCM should be specifically designed to be a multi-user distributed system that allows the authorized government users to interact in workflows. • **Secure login**: application must provide secure authorization and authentication of the application			

	users according to relevant NATO and EU standards • **Active Directory** (**AD**) must be implemented to authenticate and authorize all users and computers in a Windows domain type network - assigning and enforcing security policies for all computers and installing or updating software. • **Communication** through "B&H SDH" network: all data must be on the private network and separated from the public networks. • **Data encryption**: data in transit must be encrypted according to relevant NATO and EU standards. • **Data backup**: must be provided by means of separate device. • **Integration capabilities**: XML data import/export functionality provided by SCM to exchange data with 3rd party workflow software. **c) Administration requirements** • **User management**: application must provide user administration in form of adding, deleting, editing user accounts and passwords. • **Role management**: administrators and responsible executives must be able to assign roles to users - limiting their view and privileges according to role specification and jurisdiction. Roles must be assigned according to Law on Protection of Classified Information of Bosnia and Herzegovina (hereinafter will be referred as the Law). Administrators must have ability to edit/change roles - add or revoke privileges to some parts of application. • **User permission matrix**: allow fine grained control over document interaction modes. When user request access, classifying officials can look up the user in the SCM, add them to the access roster and assign whatever appropriate level of interaction required. This environment cross-over between the two systems is essential in providing the kind of high-availability and accuracy			

	necessary for the protection of sensitive or classified information. • **Secure editing and modification of stored documents:** Classifying officials can edit or modify document content, any changes or alterations are captured to ensure audit and oversight requirements are met. • **Document metadata search capability**: Once a document and all its relevant historical data have been entered, the full text of that metadata is searchable, thus allowing instant retrieval and review. **d) Audit requirements** • **Real-time activity tracking** of all access, review and alterations: Any interactions with documents are recorded • **Audit Reporting:** SCM should allow security officials to print detailed tracking lists, user rosters and activity reports. Any information entered during the course of its operation can be searched and retrieved for compilation into any type of report required for security handling procedure reviews or internal inspections. **Log management:** application must be able to track and list out all changes in form of report that occurred on the system i.e. certificate status change, adding new user, adding new organization, certificate expiration etc. All the items in the log must have corresponding date and user ID. **e) Security Architecture** Implemented security mechanisms have to satisfy well-known security dimensions: • Integrity: message must remain unaltered during transmission across all intermediary services, such as network devices and software components. • Confidentiality: contents of a message cannot be viewed while in transit, except by authorized			

services that need to see the message contents in order to perform routing.

- Availability: message is promptly delivered to the intended recipient, thus ensuring that legitimate users receive the services they are entitled to.
- Non-Repudiation: requestor should not be able to deny that he has requested service and Central Registry should not be able to deny that service has been provided by him.

Secondly security mechanisms to protect infrastructure elements at the Central Registry from unauthorized view or modification need to be designed. This will be done on device by device basis using well known techniques such as host hardening, enforcing strong password polices or applying ACL.

f) Securing web services

Since SSL/TLS provides confidentiality at the transport layer only, XML Encryption provides confidentiality at the application layer and thus assures end-to-end confidentiality of messages traversing multiple Web services. In order to satisfy requirements on confidentiality of the dialog, XML Encryption should be implemented at Central Registry side.

Pre-shared secrets and IPSEC VPN tunnels will be used to insure that only authorized requestors can access to Central service.

Additional layers of encryption, primarily for securing data in transit, should be realized through VPN tunnels based on IPSec protocols.

g) Source code

The owner of project source code will be MoS.

The contractor must provide full, open, paid-up, irrevocable, un-timed licenses to the proposed Software product(s) with the needed server licenses as per the requirements identified in this document. Hence the MoS shall have all rights pertaining to installing and using this Software product for an

	unlimited time period, and in any location and/or office premises. All required licenses of the commercial off the shelf proprietary software have to also be provided to the MoS. Furthermore, the software product should not have any technical or legal, built-in or inherited, limitations or constraints on the number of times or time periods and dates during which it can be used. The license will be provided and activated from the date of the operational acceptance. The full source code for any customization elements or developed modules which will enable the System to be maintained and developed with no further support from, or obligation to, the consultant provider and any additional software engineering tools and enabling technologies used to construct these applications and required to support full access to source code and development environments, are to be provided as property of MoS. **h) System Test** It is expected from the contractor to provide a system test document for all functionalities described in the detailed design document. Execution of the test cases will be done by an implementation team comprising representatives of the beneficiary institutions with the assistance of the contractor. The System test document will be reviewed by the implementation team and approved by the contracting authority. **i) Security testing** The contractor has to ensure the security of the System from potential misuse during delivery, installation and handover. It is expected from the contractor to perform technical security testing comprising of IT infrastructure and application vulnerability scanning and penetration testing. SCM should at least comply with Level 2 of OWASP Application Security Verification Standard 3.0. Testing should rely on automatic tools as well as in-depth			

	probing and evaluation using manual techniques. Security testing report should list all vulnerabilities and exploits found with indicated severity level. After fixing it, retest should be performed verifying successfulness of fixes. **4. Training** Training will be provided by the Contractor at MoS premises (Trg Bosne i Hercegovine 1, Sarajevo). Training will be consisted of user's and administrators' training. The Contractor will provide the initial staff training (10 participants) and set-up the training environment. The training will provide staff with sufficient knowledge to use the System on a daily operational basis. The Contractor shall ensure that the trainees are fully acquainted with the features and functionalities of the System as well as with its operation and maintenance. The following 10 days training activities for the administrators (3 persons) must be scheduled and coordinated with the MoS staff: • Operational procedures including Archival/Backup/Restore procedures; • Security (Access controls, Database/Document Repository and applications). Improve access control management and reports (access log, revise application controls); • Systems Management routine tasks (scheduled software maintenance, troubleshooting, maintaining logs and journals); • Use of administration/management console for management of the System configuration. As a result of the training for administrators, it is expected that the MoS will be able to maintain and operate the System independently, without the external support. 3 Days training for the users (30 persons) will consist of the following sessions, and it is expected that the training agenda will be refined during the Project implementation:			

	• Instructional session to demonstrate the functionalities and features of the System; • Hand-on exercise sessions; • Questions and answers session. Develop training materials in local language with screenshots of all user interfaces of the SCM system. The training materials must be developed in a way to support the MoS staff in conducting future trainings, according to the train-the-trainer principle. The Contractor will ensure that a detailed User Guide is provided and accessible directly from the System. Context-sensitive Help Screens are also required. The Contractor will also be responsible for developing the following training material: • Functional documentation to serve as a User Guide, demonstrating the complete usage of the System. This will be distributed to all staff using the SCM; • Trainer material, in form of presentation slides, to be used by trainers for the future trainings according to the train-the-trainer principle. Maintain and update all documentation for any changes in the System performed by the Contractor during the Contract Period and any negotiated extensions at no cost to the Purchaser or the Beneficiary (MoS). **5. Documentation** Provide (along with the System): • Detailed and updated SCM manual that covers all system management functions; • Detailed and updated electronic manual covering all user functions; • Handy guide to which all Disaster Recovery procedures are recorded, possible impact on users and the functioning of and guidance on what MoS must do to ensure the smooth flow and continued work (business continuity). The System Implementation Guide shall include, but not be limited to the following: • Detailed system design specifications;			

	• Detailed technical architecture documentation including information and diagrams that show systems, interfaces, and hardware and software architecture; • A complete description of SCM software and instruction on its operation; • Operational maintenance procedures; • Availability and Capacity Plan; • Business Continuity Plan, Backup Plan and Disaster Recovery Plan. • A screen-oriented training manual that contains all the procedures necessary for the successful operation and interaction with the SCM. **6. Project Management** It is expected from the contractor to implement a detailed Project Plan and provide manpower to execute it. **Project implementation methodology** Appoint the Lead Project Manager and the Project Team. Project teams (Contractor and MoS) will have meetings at least once in 15 days, and if necessary, more frequently. Project teams will jointly make an analysis of all requests that are the subject of procurement, consider different solutions and find the best approach and design of the system. The analysis will include technical specifications and interviews with members of the MoS project team, as well as interviews with other employees or working groups in the MoS. **7. Development of software with general functionalities** • For source code of application and queries on databases the owner will be the Ministry of Security; • Recommendation for software programming languages: VB.NET or C#.NET (due to the experience of MoS employees who will maintain			

	the system in the future • Recommendation for Database: Microsoft SQL Server Standard edition that is already installed and configuring by MoS (due to the experience of MoS employees who will maintain the system in the future); • Applications will be separated on administrator and user part; • SQL queries must not be in the source code of the application; • Compiled applications must be protected because of disabling reading the source code; • Application and all reports must be in all official languages of BiH languages Latin and Cyrillic • Communication between the client and server must be encrypted; • The data in database will be encrypted with symmetric key with AES 128 algorithm; • Avoid database queries in source code of software (application), use it only in stored procedures, triggers, views. • All activities on the application is recording by the permanent use (logs); • Application will be client-server; • Mandatory implementation Active directory and Domain Controller with integration with application; • Application can be Web or Windows based; • If Web based: ○application shall run smoothly with all latest version of web browsers like Internet explorer, Google Chrome and Firefox; ○web application needs to be developed in the way that ensures that it is readable and usable on all web browsers. **a) Login form general requirements:** • Username should be a same username that logged users use in the domain controller. • Allow users to choose the language in the forms, Bosnian (Latin), Serbian (Cyrillic) and Croatian (Latin).			

	• After the first login the entered password will be tested against all existing local accounts with the same name, and all successfully authenticated accounts will be migrated. • All user passwords has to be hashed • User and password policy must meet the following requirements: • Password complexity must be enforced (passwords must be combined of capital and small letters, numbers and other eligible characters); • Users must be forced to change password every 2 months minimum; • Users must be logged off automatically after maximum 15 minutes of inactivity; • Account lockout policy must be enabled after 3 unsuccessful logon attempts. • User must be notified in that case to contact system administrator to perform account unlock. • Disable cut/copy/paste options in the password field. **b) Logon minimum requirements** • The Host Server shall contain definitions for user names, passwords and access roles, e.g. Administrator role, Manager role, User role and Guest role. These definitions shall be local to the Host Server only and shall be inaccessible from the Client in any form. • The logon method shall be displayed at the user location. • The logon shall succeed or fail. In case of a failure, a default authentication page shall be displayed. The logon shall be capable of cancellation. • If cancelled the Home page shall be displayed. • A logon failure shall redisplay the logon method with password field blank. The password as entered shall display the character '*' in place of each password character entered.			

	c) Logout minimum requirements • After a successful login and the login page is displayed, all subsequent displayed pages shall contain a logout control. • When activated the logout control shall display a control asking for confirmation of logout. If confirmation id denied the logout confirmation is removed with no effect. If confirmed the Home Page is displayed and all subordinate windows are closed. **d) Workflow minimum requirements** • When a user performs a successful logon, the proper page shall be sent to the client allowing the displayed information to be read, entered or changed depending upon the role of the authenticated user. Further, only subordinate pages in the page hierarchy that fit the role of the user logon shall be available for viewing beginning with the Logon Home Page. **e) Administration general requirements** Administrators part will allow at least the following functionality: • Administration of system users, their access rights, accounts restrictions, etc. • Setting up a system parameters necessary for data processing: • validity of certain clearances; • degree of secrecy and their equivalents in the English language; • position and the name of the signatory on the certificates, clearances and statements; • the period of validity of storing scanned documentation on the system; The administrator enters the data of the new user and updates the information on existing users of the system.			

	User Administration must meet a minimum: • Enter the user name and password. Provide control input user name password, as follows: • Username in the database will have to first be entered in Active Directory (Domain Controller), and when entering a new user of the system will be checked the status of the user in AD. • Password must meet the following criteria: o Password complexity must be enforced (passwords must be combined of capital and small letters, numbers and other eligible characters); o Users must be forced to change password every 2 months minimum; o Users must be logged off automatically after maximum 15 minutes of inactivity; o Account lockout policy must be enabled after 3 unsuccessful logon attempts. o User must be notified in that case to contact system administrator to perform account unlock. • It should be possible password reset on the system, after which the user will receive a new password which must be changed when the first subsequent login to the system. • User is given the type of users (Administrator, users) as well as the right of access to and use of the entire system. It is necessary to allow the maximum segmentation system to enable provision or deprivation of rights, with access to every segment enable selection of the right-VIEW SELECT, UPDATE, DELETE. The minimum set of segments of the system for the user: • Security permissions (national, EU, NATO, the entry of new, print, sending requests, allocation requests in operation, the processing of requests, documentation); • Security checks (new entry, send requests, assigning work requests, requests processing and documentation).			

	• The minimum required input names, surnames and which institution-organized person belongs. • Administrator will be able to choose a language for users Bosnian (Latin) Serbian (Cyrillic) and Croatian (Latin). • It is necessary in application to have an option that will allow deactivation of account and allow limitation period of validity of account. • System access card is assigned to each user which is registered a minimum number of card and whether the card is valid or not, and further comment. Implement an interface that will allow monitoring of user activity on the system. Provide interface that will allow administrator input parameters of the system, at minimum: • Status of requests for security checking and / or the issuance of security clearances; • Types of requests, whether it is a request for a security vetting or request for the issuance of security clearances; • Types of licenses, whether it is national, NATO, EU, or, if necessary some other kind of clearances; • The reasons for rejection of the requests for the issuance of clearance and request for safety checking; • The levels of secrecy, where it will be listed degrees of secrecy and all linguistic equivalents in all official languages in Bosnia and Herzegovina, as well as the languages with which Bosnia and Herzegovina has signed security agreements on mutual exchange and protection of classified information; • Deadlines expired clearances depending on the level of classification and type of clearance; • Point out to where it will be stated period expired clearances that are required for searching and alerting the expiry of clearances;			

	• Types of users who will use the system. • Colours will be using for colouring rows in data-grid for different parameters. For example, red colour will mark all clearances have expired, orange flag all the clearances that stand out for one month, yellow colour for clearances that stand out 4 months or less from the expiration of the clearance, etc. **f) Users interfaces general requirements** Each user will be able to choose display fields to be displayed in the Data-Grid / GridView controls in certain forms in his account. Authorized users within an institution / agency may apply for security checking and issuing security clearance institutions / agencies that are under the Law responsible for safety checking and issuing security clearances. Enable autocomplete in the field of national identification number when entering to show the data corresponding to the entered part of national identification number, with simultaneously display basic personal data Name, First Name and Name of a parent, if the person is entry in the database. If there is no person has already submitted, invite form for entering a new person. Institution / agency responsible for carrying out security vettings and issuing security clearances will be used interface to review of requests and allow sending requests for further processing. When receiving the request enable printing of bar-code, which will contain a unique number (national identification number) to be printed on the printer of barcodes and stick to the subject of each person. Enable scanning supporting documentation arising during the security checking and issuance of security clearance. Scanned documents should be stored in the database or as files on disk and will be affiliated to			

	any person to which documents belong. It is necessary to allow a review of all the documentation for each person in the database. The quality of images (resolution) of scanned documents must be optimized for the database such that shall be clearly legible and usable. Resolution of scanned documents should be applicative optimized before recording in a database. During recording and using scanned documents have to separate documentation that is currently valid for a valid clearances and verification from documentation that was used for previously checking and clearance. After the end of the issuing security clearances documentation is archived and kept in the Central Registry at a specific location (shelf, closet, etc.). Filters that need to be implemented in the form of a clearance are minimal, which will search the database when you enter each character (Provide a combination of all parameters, that do not exclude each other): • Filter by national identification number, name, surname, degree of secrecy permits. • Filter by the institution where the person is employed, the type and status of the clearances, date of expiry of clearances and by authorized users who processed documentation. Enable using bar code scanner for searching with national identification number. Implement autocomplete on all fields filter/search. For every person that is subject of issuance security clearance records will be kept on the national clearances, EU and NATO clearances, as well as on the issue of NATO certificate (attestation). When entering the date of issuing the clearances, based on the degree of secrecy of the clearances, application will allow the automatic filling of the period of validity of the clearances.			

	Data on clearances for a particular person should be viewed in the same form where should be placed all the information for the person selected, the current status of clearances and checks, with the ability to preview all previous vettings and clearances. **g) Requirements for database** • All SQL database query must be in stored procedures. • All tables will have its own copy with the extension name "_History" in which to be writing the original records that are prescribed in the commands UPDATE and DELETE in stored procedures with minimum user name and date and time of a modification. All tables must be properly indexed to allow fast data searches. **h) Reports modules general features** • All reports must be in three languages: Bosnian (Latin), Serbian (Cyrillic) and Croatian (Latin). The language is selected before the printing report in particular. • All reports must be printable on any printer. • When choosing a report form allows the user that can choose report with diagram or without diagrams. The diagrams that can be selected is pie, columns, curve. • Ensure that users can choose the font that will be on the reports, as well as the size of the text and font size to titles of reports. • Enable administrators to be able to do redesign of template reports for issuing safety clearances and certificates (attestation). It is necessary to implement the production of statistical reports with charts that must offer a minimum of: • Reports and Statistical Data (monthly, semi-annual and annual) on **request** addressed to the MoS **for**			

	issuing clearance for access to classified information (CONFIDENTIAL, SECRET, TOP SECRET) for employees of certain agencies / institutions; • Reports and Statistical Data (monthly, semi-annual and annual) on the **requirements that are in the** process according to the MoS **for a issuing clearance for access to secret data** classified as CONFIDENTIAL, SECRET, TOP SECRET for employees of certain agencies / institutions, which are in operation; • Reports and Statistical Data (monthly, semi-annual and annual) of **the issued clearances for access to classified information** (CONFIDENTIAL, SECRET, TOP SECRET) by the MoS to employees in a given Agency / Institution; • Reports and Statistical Data (monthly, semi-annual and annual) of **revoked clearances for access to classified information** (CONFIDENTIAL, SECRET, TOP SECRET) by the MoS to employees in a given Agency / Institution; • Reports and Statistically Data (monthly, semi-annual and annual) **on the valid clearances for access to classified information** (CONFIDENTIAL, SECRET, TOP SECRET) for employees in some agencies / institutions; • Reports and Statistical Data (monthly, semi-annual and annual) **for clearances for access to classified information that expiry** (CONFIDENTIAL, SECRET, TOP SECRET) for employees of certain agencies / institutions. It is necessary to implement and create additional reports. • Overview of individual cards per person, that will include all similar data from the person, information about the applicable clearances and checks, as well as the history of checks and clearances. • Reports on the number of valid, cancelled, invalid, expired clearance with the option of grouping by the degree of secrecy, type of clearance, period of			

	issuance, annulment, type of clearance, institutions / agencies and years. • Review of requests sent to vetting and requests for clearance issuing, and separate ones are sent to procedures and ones are in process and ones are completed. **System Test:** Provide a system test document for all functionalities described in the detailed design document. Execution of the test cases will be done by an implementation team comprising representatives of the beneficiary institutions with the assistance of the contractor. The System test document will be reviewed by the implementation team and approved by the contracting authority. **Security testing:** Ensure the security of the System from potential misuse during delivery, installation and handover. It is expected from the contractor to perform technical security testing comprising of IT infrastructure and application vulnerability scanning and penetration testing. Delivery, installation and assembly and integration with other parts of the system (Items number: 1.7, 1.8, 1.10, 1.11, 1.13, 1.15, 1.16).			
	CONSUMABLES **1. Sets of full load paper for printing for Barcode label printer, Item 1.2** Original sets of full load paper for printing for compatible with Barcode label printer, Item 1.2 **QTY: 10 sets** **2. Sets of original full toner set for Laser printer, item 1.15** Original sets of full toner set for printing compatible with Laser Printer, Item 1.15 **QTY: 10 sets**			

	List of Abbreviations
ARP	Address Resolution Protocol
DDoS	Distributed Denial of Service
DDR	Double Data Rate
DIMM	Dual In-Line Memory Module
DNS	Domain Name System
DoS	Denial of Service
DVI	Digital Visual Interface
ECC	Error-Correcting Code
Gbps	Gigabits per second
GUI	Graphical User Interface
HBA	Host Bus Adapter
HDMI	High-Definition Multimedia Interface
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security

	List of Abbreviations
KVM	Keyboard Video Mouse
LRDIMM	Load-Reduced DIMM
MoS	Ministry of Security
OS	Operating System
PCL	Printer Command Language
PDU	Power Distribution Unit
RAID	*Redundant Array of Independent Disks*
RDIMM	Registered DIMM
SAS	Serial Attached SCSI
SATA	Serial Advanced Technology Attachment
SDRAM	Synchronous Dynamic Random-Access Memory
SFF	Small Form Factor
SFP	Small Form-Factor Pluggable
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
SSD	Solid State Drive
SSL	Secure Socket Layer
TLS	Transport Layer Security

	List of Abbreviations
USB	Universal Serial Bus
UTP	Unshielded Twisted Pair
VGA	Video Graphics Array
VM	Virtual Machine
VPN	Virtual Private Network
WSDL	Web Services Description Language
XML	EXtensible Markup Language

Places of delivery are as follows:

Item	Type	Institutions for delivery	Total Qty	
1.1	Cabling	Ministry of Security	350 m	
1.2	Barcode Label printer	Ministry of Security	2	5
		State Agency for Investigation and Protection	1	
		Ministry of Defence	1	
		Intelligence-Security Agency	1	
1.3	Laser Barcode Scanner	Ministry of Security	9	30
		State Agency for Investigation and Protection	8	
		Ministry of Defence	6	
		Intelligence-Security Agency	7	
1.4	Firewall type 1	Ministry of Security	2	
1.5	Firewall type 2	State Agency for Investigation and Protection	1	3
		Ministry of Defence	1	
		Intelligence-Security Agency	1	
1.6	Network switch	Ministry of Security	2	
1.7	Servers Type 1	Ministry of Security	2	
1.8	Servers Type 2	State Agency for Investigation and Protection	1	2
		Ministry of Security	1	
1.9	SAN switch	Ministry of Security	1	
1.10	Storage	Ministry of Security	1	
1.11	Desktops	Ministry of Security	9	30
		State Agency for Investigation and Protection	8	
		Ministry of Defence	6	
		Intelligence-Security Agency	7	
1.12	UPS	Ministry of Security	2	

1.13	Fast document scanner	Ministry of Security	2	5
		State Agency for Investigation and Protection	1	
		Ministry of Defence	1	
		Intelligence-Security Agency	1	
1.14	Server Rack Cabinet	Ministry of Security	1	
1.15	Laser Printer	Ministry of Security	2	5
		State Agency for Investigation and Protection	1	
		Ministry of Defence	1	
		Intelligence-Security Agency	1	
1.16	Virtualization Software	Ministry of Security	1	
1.17	Software, database and reports development, installation, configuration and integration with installed system	Ministry of Security	1	
		State Agency for Investigation and Protection		
		Ministry of Defence		
		Intelligence-Security Agency		

Addresses:

Ministry of Security	Trg BiH 1, Sarajevo
Ministry of Defence	Hamdije Kreševljakovića 98, Sarajevo
Intelligence-Security Agency	Mehmeda Spahe 7, Sarajevo
State Agency for Investigation and Protection	Nikole Tesle 59, East Sarajevo