Annex No. 1 to Ref. No. PPR-12120-22/ČJ-2013-990656

Technical specifications for the project "Development of consolidated IT infrastructure of Police of Czech Republic - BACKUP CENTER"

Police of the Czech Republic operates the fragmented structure of infrastructure platforms and resources for individual information systems. These information systems are run on different hardware (different types of servers) and software (operating and database systems) platforms. Their management is a complex and requests high number of specialists for service staff and is costly as for the operation.

To ensure the reduction of the operating costs of IT infrastructure Police decided to consolidate the operation of information systems and to eliminate the above shortcomings and at the same time to ensure the necessary flexibility in the allocation of infrastructure resources. Future goal is a state where end users are provided with a service infrastructure and resources in measurable quality. The first step to the future objective is to ensure a robust infrastructure platform, including required software, which covers the subject of this contract.

In order to ensure high data availability Police operates two data centres in geographically separated locations that are functionally equivalent and mutually backed up.

The project „Development of consolidated IT infrastructure of Police of Czech Republic - BACKUP CENTER" addresses the recovery of the IT infrastructure in the backup location and is directly linked to the project prepared under the Swiss-Czech Cooperation entitled "Development of consolidated IT infrastructure of Police of Czech Republic".

The offer of the applicant must be integration into SAN infrastructure without having to disconnect the device (the HA mode) and also a possible upgrade of components (firmware upgrade). Given that it is only a supplement and extension of existing consolidated ITC infrastructure, the supplier must fully accept requirements for an existing consolidated infrastructure and proposed components must be fully compatible with this newly built consolidated infrastructure. In this context, the contracting authority requires confirmation from the manufacturer of equipment for LAN networks, that the applicant is entitled to install, service and upgrade devices that are associated with the installation of the LAN. Namely SAN and LAN networks is the HP 3PAR V800, HP 6600-24G-4XG, HP 7506, HP F1000-EI, HP Blade System C7000, HP Blade Server 460c G6 and G7. Contracting authority also requires a

supplier's declaration that offered components are fully compatible with the devices described in the preceding sentence.

Basic bloc of the project – public contract

List of items according to the technical specifications of public contract:

Item number	Item name	Number of items
Block 1	**Delivery of hardware products**	
1.1	Cabinet for placement of hardware components (rack)	1 pc
1.2	Server rack for blade servers (blade chassis)	1 pc
1.3	Set – application blade server x86	4 pcs
1.4	Set – application blade server x86 extended RAM	2 pcs
1.5	Set – database blade server UNIX	2 pcs
1.6	Specialized solution to protect against security threats and vulnerabilities of systems and applications - System NG-IPS	1 pc
1.7	Expansion of disc field 3Par	1 pc
Block 2	**Delivery of SW products**	
2.1	Virtualization SW	12 pcs
2.2	SW for the administration of HW and delivery of infrastructure as a service	1 set
2.3	Other software	Set of licences
Block 3	**Integration and consulting services**	
3.1	Drafting of the proposal of the architecture and operation of high availability between two data centres in the consolidated infrastructure under this contract and the previous stage in the primary centre.	
3.2	Implementation and configuration work in constructing of consolidated infrastructure and integration into existing infrastructure of Police of Czech Republic	

Technical specification of different block of the solutions – public contract

Podpořeno z Programu švýcarsko-české spolupráce
Supported by a Swiss-Czech Cooperation
programme

Annex No. 1 to Ref. No. PPR-12120-22/ČJ-2013-990656

Block 1 Delivery of HW products

1.1 Cabinet for placement of hardware components (rack)		1 pc
Item	**Requested**	**Value offered by the applicant**
Height	42 U	
Mark – type	-	
Depth	sufficient for all the components supplied, min. 80 cm	
Design	front and rear doors with horizontal ventilation	
Accessories	rack KVM console (max. 1U, 17´´monitor, keyboard, positioning device)	
	Side panels	
	2 x PDU (min 40A) for redundant connection of sources of chassis to two independent inputs	
Guarantee	min. 3 years on all components with the response of four hours in the solution, cover 24 x 7;	

1.2 Server rack for blade servers (blade chassis)		1 pcs
Item	**Requested**	**Value offered by the applicant**
Design	Rack and 100% compatible with the blade servers specified below under "1.3 Set – application blade server x86", "1.4 Set – application blade server x86 extended RAM" and "1.5 Set – database blade server UNIX". Enabling joint installation of further demanded and already operated servers for redundant connecting of all LAN and FC ports	
depth inside	min. 14 active positions for half-height blade servers. Active position means	

Podpořeno z Programu švýcarsko-české spolupráce
Supported by a Swiss-Czech Cooperation
programme

Annex No. 1 to Ref. No. PPR-12120-22/ČJ-2013-990656

	that when you insert an additional server you will not need to buy and add nothing and server will work. The requirement can be met by installing 2 blade chassis.	
Power supply	Hot-plug sources for ensuring of redundant operation of fully wired chassis	
Ventilators	Hot-plug ventilators for ensuring of redundant operation of fully wired chassis	
Management	Redundant	
LAN connectivity	2 x 10Gb Ethernet module enabling HW distribution of server network cards, and each at least for 4 separate sites presented to servers, Every Ethernet module will be wired by 4 x 1Gb RJ45 a 2 x 10Gb SFP+ module	
FC connectivity	2 x Storage Area Network 8 Gb/s interconnect module (8 external ports incl. short wave 8Gb SFP, number of internal ports must correspond with number of servers configurable into blade chassis, web interface for administration, licences for all ports)	
Remote management	by LAN (option to disconnect power supply, 128-bit encryption, monitoring of hardware with no operating system installed) possibility of setup and control of multiple server racks from one place monitoring and reporting of information on the operating temperature and power consumption of each server or rack in real-time built-in display for easy operation integrated and coherent approach to management processors of all servers in the rack	

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Podpořeno z Programu švýcarsko-české spolupráce
Supported by a Swiss-Czech Cooperation
programme

Annex No. 1 to Ref. No. PPR-12120-22/ČJ-2013-990656

	single sign-on access to all devices in the rack. asset management of all devices in the frame of the rack	
Installation	HW installation, complete setting into operation and activation	
Guarantee	• min. 3 years on all components • action during 4 hours on the place of the performance • cover 24 x 7 • regular checks of HW • preparation of reports on incidents • support of the deployment of new versions of FW and SW • regular consultation with the technical representative of the manufacturer	

1.3 Set – application blade server x86		4 pcs
Item	**Requested**	**Value offered by the applicant**
Requests for CPU by tests of SPEC CPU2006		
SPECint_2006	**min. 43,2**	
SPECfp_2006	**min. 71,2**	
SPECint_rate 2006	**min. 436**	
SPECfp_rate 2006	**min. 357**	
Mar – type of server	-	
Design	to requested blade chassis	
Processor	-	
	Min. number – 2	
Memory	96 GB RAM DDR3 1333MHz	
Internal storage area	min. 2 GB USB flash or SD card for hypervisor installation	
Sequence switch	HW RAID 0,1; 512 GB Cache	
Network adapter	2 x 10 Gb/s TCP/IP Offload Engine;	

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Podpořeno z Programu švýcarsko-české spolupráce
Supported by a Swiss-Czech Cooperation
programme

Annex No. 1 to Ref. No. PPR-12120-22/ČJ-2013-990656

	every one with the option of distribution on HW level up to 4 virtual adapters	
FC interface	Two-ports Fibre Channel 8Gb adapter, SW for redundant connection of the server with MS Windows 2008/2003 for delivered disc area	
Monitoring of HW	Integrated directly in hardware components without installing of agents into the operating system	
Remote management	by LAN (graphic console also without installed OS, possibility to disconnect power supply, reset of the system, keyboard, mouse, 128-bit encryption, monitoring of hardware with no operating system installed) Software for remote administration must allow: centralized remote management of hardware and gathering of information about the configuration and status of server hardware components (including storing such information in a database for further use), detection and messaging (at least using SNMP protocol) on error conditions	
Compatibility	Microsoft Windows 2008/2012, Red Hat EL4, SuSe Linux, VMWare ESX 4.x, 5.x	
Installation	HW installation, complete setting into operation and activation	
Guarantee	min. 3 years for all components • action during 4 hours on the place of performance • cover 24 x 7 • regular check of state of HW • preparation of reports on incidents • support of the deployment of new versions of FW and SW • regular consultation with the technical representative of the manufacturer	

Podpořeno z Programu švýcarsko-české spolupráce
Supported by a Swiss-Czech Cooperation
programme

Annex No. 1 to Ref. No. PPR-12120-22/ČJ-2013-990656

1.4 Set – application blade server x86 extended RAM		2 pcs
Item	**Requested**	**Value offered by the applicant**
Requests for CPU by tests SPEC CPU2006		
SPECint_2006	**min. 43,2**	
SPECfp_2006	**min. 71,2**	
SPECint_rate 2006	**min. 436**	
SPECfp_rate 2006	**min. 357**	
Mark - type of the server	-	
Design	into the requested blade chassis	
Processor	-	
	Min. number – 2	
Memory	128 GB RAM DDR3 1333MHz	
Internal storage area	min. 2 GB USB flash or SD card for the hypervisor installation	
Sequence switch	HW RAID 0,1; 512 GB Cache	
Network adapter	2 x 10 Gb/s TCP/IP Offload Engine; every one with the option of distribution on HW level up to 4 virtual adapters	
FC interface	Two-ports Fibre Channel 8Gb adaptor, SW for redundant connection of the server with MS Windows 2008/2003 for delivered disc area	
Monitoring of HW	Integrated directly in hardware components without installing of agents into the operating system	
Remote management	by LAN (graphic console also without installed OS, possibility to disconnect power supply, reset of the system, keyboard, mouse, 128-bit encryption, monitoring of hardware with no operating system installed	

Annex No. 1 to Ref. No. PPR-12120-22/ČJ-2013-990656

	Software for remote administration must allow: centralized remote management of hardware and gathering of information about the configuration and status of server hardware components (including storing such information in a database for further use), detection and messaging (at least using SNMP protocol) on error conditions	
Compatibility	Microsoft Windows 2008/2012, Red Hat EL4, SuSe Linux, VMWare ESX 4.x, 5.x	
Installation	HW installation, complete setting into operation and activation	
Guarantee	min. 3 years for all components • action during 4 hours on the place of performance • cover 24 x 7 • retention of defective discs with contracting authority • regular check of state of HW • preparation of reports on incidents • support of the deployment of new versions of FW and SW • regular consultation with the technical representative of the manufacturer	

1.5 Set – database blade server UNIX		2 pcs
Item	Requested	
Mark - type of the server	-	
Design	into the requested blade chassis	
Processor	64 Bit RISC/EPIC Processor min. 8 of cores (2 GHz)	
	Number of configurable CPU: min. 2 pcs	
Memory	48 GB RAM DDR3 1333MHz	

Internal storage area	2x 146GB 6G SAS 15krpm	
Sequence switch	HW RAID 0,1; 512 GB Cache	
Network adapter	4 x 10 Gb/s TCP/IP Offload Engine; every one with the option of distribution on HW level up to 4 virtual adapters	
FC interface	Two-ports Fibre Channel 8Gb adaptor, SW for redundant server connections for delivered disc area	
Remote management	by LAN (graphic console also without installed OS, possibility to disconnect power supply, reset of the system, keyboard, mouse, 128-bit encryption, monitoring of hardware with no operating system installed Software for remote administration must allow: centralized remote management of hardware and gathering of information about the configuration and status of server hardware components (including storing such information in a database for further use), detection and messaging (at least using SNMP protocol) on error conditions	
OS	UNIX including cluster licenses compatible with used HP-UX SW	
Virtualization	In the frame of the physical server the system must ensure operating of virtual servers, each with its own instance of the OS, host name and IP address. Virtualization technology must be recognized as a "hard partitioning" for Oracle products	
Installation	HW installation, complete setting into operation and activation	
Guarantee	min. 3 years for all components • action during 4 hours on the place of performance • cover 24 x 7 • regular check of state of HW • preparation of reports on	

Podpořeno z Programu švýcarsko-české spolupráce
Supported by a Swiss-Czech Cooperation
programme

Annex No. 1 to Ref. No. PPR-12120-22/ČJ-2013-990656

	incidents • support of the deployment of new versions of FW and SW • regular consultation with the technical representative of the manufacturer	

1.6 Specialized solution to protect against security threats and vulnerabilities of systems and applications - System NG-IPS

For the completion of the system of the security of perimeter, demilitarized zones and the selected virtual networks it is necessary to deploy in-line NG-IPS for data lines. NG-IPS must with a minimum of added delays inspect communications and automatically block objectionable network traffic. This all with providing of clear information to security analysts of the network administration and reporting to superior SIEM application.

Main requested services of the system NG-IPS:

1. ***Standard set of functions of 1st generation IPS*** – to provide transparent protection against vulnerabilities and exploits with the integration of the on-road communication inspection (in-line).
2. ***Knowledge and visibility into application*** – ability to identify malicious applications and to enforce security policies on application layer regardless of port or protocol used.
3. ***Context awareness –*** ability to include into deciding on blocking information from external sources and to apply the decision having regard to the geographic location of the network transaction partner, its reputation and possible information from directory services.
4. ***Content awareness*** – ability to control and sort incoming and outgoing files, commands, and to generally understand the content with the hyperlinked structure.
5. ***Preparedness for security developments*** – to support the options to upgrade to new technologies that will address the future threats.

General characteristics and qualities required from NG-IPS solutions
▪ Protection against security threats and vulnerabilities of systems and applications
▪ Protection against DoS and DDoS
▪ Equivalent support of IPv4 and IPv6
▪ Protection by reputation service (Rep DV) with geographic system of recognition of resource
▪ Broad and accurate security with limiting of false alarms

Podpořeno z Programu švýcarsko-české spolupráce
Supported by a Swiss-Czech Cooperation
programme

Annex No. 1 to Ref. No. PPR-12120-22/ČJ-2013-990656

- ▪ Integration of functions of Next-Gen Firewalls – recognition and visibility into applications
- ▪ Support of inspection in heterogeneous environment regardless of the manufacturer of network infrastructure
- ▪ Support of inspection in a virtualized environment
- ▪ Possibility of high availability solutions to prevent network downtime
- ▪ Scalable performance and minimal added delay
- ▪ Intuitive controls - easy to learn and reliable to use
- ▪ Surveillance management console NG-IPS for redundant solution or for virtual environment vSphere
- ▪ Technical support 24*7*365 as the basis for 3 years

Description of requirements for the system NG-IPS with the output of min. 700Mbit/s:

System NG-IPS		1 pcs
Required functionality	Requirement specification	Value offered by the applicant
Aggregated throughput NG-IPS at full load with all filters turned on certified by independent testing organizations ICSA Labs, Tolly Group or NSS	min. 700 Mbit/s	
Minimum total number of segments for in-line inspection (can be a combination of 10/100/1000 Base-T and SFP)	10 x 1GE segments	
The device must support the types of SFP ports without the need for external converters	1000 Based UTP SFP	
	1000 Based-SX SFP	
	1000 Based-LX/LH SFP	
The maximum delay of NG-IPS at full load with all filters turned on certified by independent testing organizations ICSA Labs, Tolly Group or NSS	< 80 microsecond.	
Number of inspected connections in real time	min. 6 000 000	
The amount of newly opened connections per second, inspected at NG-IPS	min. 110 000 connections/s	
Support of SYN-Proxy	min. 300 000 connections/s	
Required inspection of transport systems	VLAN 802.1Q, VLAN QinQ 802.1ad, GRE, MPLS, IPv4, IPv6	
Redundant hot-swap power supply in the base	IS SUPPORTED	

Annex No. 1 to Ref. No. PPR-12120-22/ČJ-2013-990656

High availability in the mode	Active-Active	
	Active-Passive	
L2 Fallback Support for internal software errors, or congestion of the system	IS SUPPORTED	
Support of Zero Power High Availability (ZPHA) for optical and also metallic ports	IS SUPPORTED	
The part of delivery is solution for ZPHA metallic ports - 5 segments	IS SUPPORTED	
Support for asymmetric operations (equipment may not within the inspection segment see in both directions of TCP connections - typically the Link Aggregation) and support of asymmetric inspection (different configurations of NG-IPS security profiles for different direction within the inspection segment)	IS SUPPORTED	
Support for the function of Adaptive filter configuration that warns or shuts down inefficient filter, which can cause congestion of the system	IS SUPPORTED	
Support of Hitless upgrade of the operation system NG-IPS without necessity of scheduling of downtime of the system, support of Hitless reboot.	IS SUPPORTED	
NG-IPS must contain filters / signatures describing	exploits, vulnerabilities, identity theft, spyware, viruses, exploration activities, protection of the network infrastructure, IM applications, P2P networks and tools to control the flow of multimedia	
Support of automatic updates of filters / signatures and databases IPv4, IPv6 and DNS of system names on Internet with damaged reputation. Automatic updates must be performed at least 2 times a week.	IS SUPPORTED	
Database IPv4, IPv6 and DNS names must allow sorting by country of origin of IP address, potential hazards and the type of hazard identified	IS SUPPORTED	

Podpořeno z Programu švýcarsko-české spolupráce
Supported by a Swiss-Czech Cooperation programme

Support of the application for writing of custom filters	IS SUPPORTED	
Support of importing of community filters / signatures Snort	IS SUPPORTED	
Minimal set of required actions of NG-IPS after the filter action: Block (Drop Packet), Block (TCP Reset), Permit, Trust, Notify, Trace (Packet Capture), Rate Limit and Quarantine	IS SUPPORTED	
Support of the translation of 802.1Q in the frame of the security segment, for inspecting the inner VLAN without the need to engage the device to all physical paths where is desired the inspection of the operation.	IS SUPPORTED	
NG-IPS must be able to detect and block attacks of exploration activities	IS SUPPORTED	
NG-IPS must support adaptive filter protection against overload or DoS attack against NG-IPS	IS SUPPORTED	
NG-IPS must be able to detect and block attacks on the basis of IP address, or DNS name "known bad host" such as spyware, phishing or Botnet C&C	IS SUPPORTED	
NG-IPS must be able to recognize traffic based on Geo-location and be able to block or apply different security packages on traffic by the detection of the geographical origin of the source IP address	IS SUPPORTED	
Possibility of limiting and limiting of bandwidth for streamed multimedia and P2P networks	IS SUPPORTED	
NG-IPS must be able to detect and block attacks against network infrastructure of the company, such as switches, routers, firewall, wireless switches and the like. It must also provide protection for the protocols used in IP telephony	IS SUPPORTED	
NG-IPS must be fully transparent to the existing network environment and its use should not be subject to the reconfiguration of existing active	IS SUPPORTED	

elements		
Support of SNMPv3, private MIB, Syslog-NG, SNMP Trap	IS SUPPORTED	
NG-IPS must be manageable from the central monitoring and configuration system (central monitoring console), but in the case of system failure must allow configuration changes without supervisory tools through web/SSL interface NG-IPS	IS SUPPORTED	

Description of the requirements for the control system (monitoring console) for delivered NG-IPS:

Requested	Value offered by the applicant
Central monitoring console must be able to manage more NG-IPS – minimally 10	
Central monitoring console must have the possibility of service from operation systems Linux, Microsoft and Mac-OS	
Central monitoring console must be in redundant design with full resistance to failure of any component or must be in the virtual design for the environment VMWARE vSphere	
Central monitoring console must be able to provide updating and distribution of filters / signatures automatically, manually and on time schedule	
Central monitoring console must be able to maintain and manage the Operating System NG-IPS	
Central monitoring console must support minimally 100 million logs in the Event log.	
Central monitoring console must be able to generate reports manually and on time schedule for categories All attacks, Specific & Top N attack, Source, Destination, Misuse and Abuse report, Rate limiting report, Traffic Threshold report, Device Traffic Statistics and Advance DDoS report	
Central monitoring console must be able to export reports to formats such as PDF, HTML, CSV, XML etc.	
Central monitoring console must be able to integrate with Microsoft AD to create security profiles for users and groups of users.	
Central monitoring console must be able to integrate with Microsoft AD for finding of users in Event log.	
Central monitoring console must support Syslog NG (syslog on TCP, incl. encryption support)	

Annex No. 1 to Ref. No. PPR-12120-22/ČJ-2013-990656

1.7 Capacity expansion of the existing disk array and promotion of the functionality

Due to maximum use of existing technologies, including the use of invested funds, we require to use as a data space for the required solutions the existing disc array HP 3PAR T800. In the frame of this project we want to upgrade capacity of the array, thus increasing gross array capacity, and functional upgrade, i.e. delivery of the relevant licenses.

Capacity expansion of the existing disk array and promotion of the functionality		1 pcs
Item	**Requested**	**Value offered by the applicant**
Design	Disc magazines (HDD) to existing disc array HP 3PAR T800 incl. SW license for the administration of the required capacity	
Disc space no.1 – capacity	Requested 4,8 TB of rough capacity	
Disc space no.1 - parameters of HDD	300 GB FC 15k	
Disc space no.2 – capacity	Requested 16 TB of rough capacity	
Disc space no.2 - parameters of HDD	1 TB SATA 7,2k	
Promotion of functionality – required licenses	SW HP 3PAR RemoteCopy license for delivered capacity SW for integration with vSphere and Vcenter server	
Installation	HW installation, complete setting into operation and activation	
Guarantee	min. 3 years for all components with the service ensuring: - Commitment to resolve hardware problems within six hours - Immediate response / intervention for critical issues - Dedicated spare parts	

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Podpořeno z Programu švýcarsko-české spolupráce
Supported by a Swiss-Czech Cooperation
programme

Annex No. 1 to Ref. No. PPR-12120-22/ČJ-2013-990656

	- Assigned client support team	
	- Assigned support manager	
	- Assigned HW and SW specialist	
	- Plan of technical support	
	- Technical verification of high-availability of disc array	
	- Update of storage Micro-code	
	- Electronic support	
	- Software update	
	- Check of operating conditions	
	contractor does not require return of the defective HDD	

Block 2 – Delivery of SW products

2.1 Virtualization SW		12 pcs
Item	**Requested**	**Value offered by the applicant**
Design	software – license for CPU	
Parameters	Auto balancing of performance between physical servers. Move of virtual servers during the operation according to their workload and performance needs of HW. Automatic start-up of virtual servers in case of failure of a physical server	
	Implemented virtualization system management from one centre, inclusion in existing management of virtualization solution that is implemented by the product VMware vCenter Server.	

Annex No. 1 to Ref. No. PPR-12120-22/ČJ-2013-990656

	Function of higher availability - virtual server can have running a backup copy on another HW server. In case of emergency of primary HW server there will be automatically activated uninterruptable backup copy	
	Functionality of virtual distributed switch	
Installation	SW installation, complete setting into operation and configuration	
Guarantee	min. 1 year of SW support of the product	

2.2 SW for the administration of HW and delivery of infrastructure as a service		1 set
Item	Requested	**Value offered by the applicant**
Design	Software	
Parameters, function and features of software	Management not just of the chassis, its resources, or fans, but also all other installed components – servers, Ethernet and FC switches	
	Integrated support for the administration and supervision of virtual servers installed on the platform VMware vSphere (incl. integration with vCenter) and MS Hyper-V (incl. integration with MS SCVMM)	
	storing of information into locally placed db MS SQL (db itself is on SQL server in the location, not on local drives of the server where the software will be installed for remote management)	
	option to install the server instance for each data centre and one server that would control	
	Option of installation in HA mode	
	management of access rights to the central part of SW and to management tools using accounts of domain Active Directory	

	only fully graphical interface to manage all installed components (servers, switches, power supplies, fans), including the possibility of transition to a fully graphical console of each server	
	Creating and storing of the definitions of "logical servers", which will be able to run in a virtual environment or on a physical server. These definitions of logical servers must then be transferable from one physical server to another by simply going to move the load on the server with different hardware configuration	
	SW must ensure so-called drag & drop management of "logical server profiles" and their transfer to any physical or virtual server without impacting the LAN and SAN infrastructure outside the server rack (i.e. unchanged on top of rack elements or story elements)	
	Logical server profile must minimally solve definition of MAC and WWN for servers (i.e. virtualization of LAN and SAN interface), connection to the existing LAN (the definition of VLAN and port mirroring will do) and SAN (incl. FC boot parameters) infrastructure	
	Views and active management of virtual and physical servers from a single console, as well as the management of stored definitions of logical server profile	
	Support of the creation of "list of IT resources" at the level of both physical and virtual servers, physical and virtual storages, network sources (e.g. VLAN), image OS/applications.	
	Creating standard pre-built installations that are accessible through self-service portal as automatic installation. Enables distributed deployment	
	SW must enable standardization of IT at the level of "patterns" using elements promoted in the "List of IT resources"	

	Defining of patterns in an integrated graphical environment and automatic generation of scripts to implement these patterns	
	The ability to assign accounting / financial values for the various "patterns", respectively. for each "IT resources" used in the "pattern"	
	Interface enabling to integrate with existing tools and processes, such as change management, service catalogue	
	Possibility of simple DR solution for both physical and virtual servers between two sites for non-critical processes without the use of cluster services	
	Integration with software HP System Insight Manager used for the HW monitoring of x86 infrastructure	
Installation and additional services	SW installation, complete setting into operation and configuration incl. following services: • pre-installation preparation and consultation, environmental control, preparation of configuration • complete installation of HW and complete installation of SW for the administration • inclusion in the software for remote administration of the existing environment of x86 servers • integration of existing blade infrastructure HP c7000 and BL460 into offered SW for remote administration • firmware upgrades of HW • complex system check for SW min. once a year • regular proactive check of the environmental compatibility (proactive notification of new tested firmware and drivers) • configuration and customization of the whole solution	
Guarantee	min. 3 years for all components with the service ensuring the following: • Software support - immediate response for critical defects,	

	in all other cases the response of two hours, - Assigned support team (assigned support manager, assigned support HW specialist, assigned support SW specialist), - Regular planning of support and activities according to records in the technical plan, - Operating quarterly meetings, - Report overview of activities of technical support quarterly, - Check of the status of the system (for servers) once a year, - Analysis of the operation system and management of repair modules quarterly, - Electronic support, a comprehensive source of electronic information, tools and services as well as self-help tools, forums, and access to the most comprehensive multi-supplier, multi-platform IT information database, - Accelerated escalation processes and elevation of problems, - Dedicated spare parts, - Flexible reporting of defects (telephone, e-mail, web), - Operator training for basic management of acquired software - Assistance in creating a plan for future advanced training	

2.3 Other SW		Set of licences
Item	Requested	
Design	software – licence, latest current revision at the date of the competition	
Parameters	9x Microsoft SQLSvrEntCore OLP 2 Lic NL Gov CoreLic Qlfd (2core licence)	

Podpořeno z Programu švýcarsko-české spolupráce
Supported by a Swiss-Czech Cooperation
programme

Annex No. 1 to Ref. No. PPR-12120-22/ČJ-2013-990656

	6 x Microsoft OS Windows Server (each license shall contain an unlimited number of virtual licenses)	
	2 x license for web SW Microsoft SharePoint Server Enterprise Edition	
Installation	SW installation, complete setting into operation and configuration	

Block 3 Integration and consulting services

Contracting Authority further requires having as the part of the delivery the related services that will lead to the fulfilment of the objectives set at the outset of technical specifications, namely:

3.1 Drafting of the proposal of the architecture and operation of high availability between two data centres in the consolidated infrastructure under this contract and the previous stage in the primary centre

- Preparation of draft of the architecture of consolidated infrastructure in the backup data centre, including detailed technical design of the solution in a backup location

- Drafting of the proposal of the architecture and operation of high availability between two data centres in the consolidated infrastructure under this contract and the previous stage in the primary centre.

3.2 Implementation and configuration work in constructing of consolidated infrastructure and integration into existing infrastructure of Police of the Czech Republic

- Preparation of a detailed technical design of solutions for specialized protection against attacks

- Technical project of the integration of delivered components to ICT environment of Police of the Czech Republic

- Physical installation of supplied components into the environment of the backup centre (or even primary centre based on the approved architecture design and technical project)

- Activation of delivered components

- Installation of SW

Podpořeno z Programu švýcarsko-české spolupráce
Supported by a Swiss-Czech Cooperation
programme

Annex No. 1 to Ref. No. PPR-12120-22/ČJ-2013-990656

- Configuration of components (HW, SW) by technical project

- Setting of environment in the primary and backup location for a high availability

- Integration with existing systems of ICT of Police (especially backup, infrastructure monitoring)

- Design of tests defined in technical project

- Documentation of environment