TECHNICAL SPECIFICATION

CYBER SECURITY MONITORING CENTRE

Functional Details of overall system:

1	Inventory of Authorized and Unauthorized Devices	Compliance
(a)	Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization's public and private network(s). Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.	To be demonstrated by vendor & checked by BOO
(b)	If the organization is dynamically assigning addresses using DHCP, then deploy dynamic host configuration protocol (DHCP) server logging, and use this information to improve the asset inventory and help detect unknown systems.	
(c)	Ensure that all equipment acquisitions automatically update the inventory system as new, approved devices are connected to the network.	
(d)	Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc. The asset inventory created must also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organization's network.	
2	**Inventory of Authorized and Unauthorized Software**	
(a)	Devise a list of authorized software and version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified.	To be demonstrated by vendor & checked by BOO
(b)	Deploy application white listing technology that allows systems to run software only if it is included on the white list and prevents execution of all other software on the system. The white list may be very extensive (as is available from commercial white list vendors), so that users are not inconvenienced when using common software. Or, for some special-purpose systems (which require only a small number of programs to achieve their needed business functionality), the white list may be quite narrow.	
(c)	Deploy software inventory tools throughout the organization covering each of the operating system types in use, including servers, workstations, and laptops. The software inventory system should track the version of the underlying operating system as well as the applications installed on it. The software inventory systems must be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.	
(d)	Virtual machines and/or air-gapped systems should be used to isolate and run applications that are required for business operations but based on higher risk should not be installed within a networked environment.	
3	**Secure Configurations for Hardware and Software**	
(a)	Establish standard secure configurations of your operating systems and software applications. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.	To be demonstrated by vendor & checked by BOO
(b)	Follow strict configuration management, building a secure image that is used to build all new systems that are deployed in the enterprise. Any existing system that becomes compromised should be re-imaged with the secure build. Regular updates or exceptions to this image should be integrated into the organization's change management processes. Images should be created for workstations, servers, and other system types used by the organization.	
(c)	Store the master images on securely configured servers, validated with integrity checking tools capable of continuous inspection, and change management to ensure that only authorized changes to the images are possible. Alternatively, these master images can be stored in offline machines, air-gapped from the production network, with images copied via secure media to move them between the image storage servers and the production network.	
(d)	Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.	

(e)	Use file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered. The reporting system should: have the ability to account for routine and expected changes; highlight and alert on unusual or unexpected alterations; show the history of configuration changes over time and identify who made the change (including the original logged-in account in the event of a user ID switch, such as with the su or sudo command). These integrity checks should identify suspicious system alterations such as: owner and permissions changes to files or directories; the use of alternate data streams which could be used to hide malicious activities; and the introduction of extra files into key system areas (which could indicate malicious payloads left by attackers or additional files inappropriately added during batch distribution processes).	To be demonstrated by vendor & checked by BOO
(f)	Implement and test an automated configuration monitoring system that verifies all remotely testable secure configuration elements, and alerts when unauthorized changes occur. This includes detecting new listening ports, new administrative users, changes to group and local policy objects (where applicable), and new services running on a system. Whenever possible use tools compliant with the Security Content Automation Protocol (SCAP) in order to streamline reporting and integration.	
(g)	Deploy system configuration management tools, such as Active Directory Group Policy Objects for Microsoft Windows systems or Puppet for UNIX systems that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals. They should be capable of triggering redeployment of configuration settings on a scheduled, manual, or event-driven basis.	
4	**Continuous Vulnerability Assessment and Remediation**	
(a)	Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator along with risk scores that compare the effectiveness of system administrators and departments in reducing risk. Use a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project).	To be demonstrated by vendor & checked by BOO
(b)	Correlate event logs with information from vulnerability scans to fulfill two goals. First, personnel should verify that the activity of the regular vulnerability scanning tools is itself logged. Second, personnel should be able to correlate attack detection events with prior vulnerability scanning results to determine whether the given exploit was used against a target known to be vulnerable.	
(c)	Perform vulnerability scanning in authenticated mode either with agents running locally on each end system to analyze the security configuration or with remote scanners that are given administrative rights on the system being tested. Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses. Ensure that only authorized employees have access to the vulnerability management user interface and that roles are applied to each user.	
(d)	Subscribe to vulnerability intelligence services in order to stay aware of emerging exposures, and use the information gained from this subscription to update the organization's vulnerability scanning activities on at least a monthly basis. Alternatively, ensure that the vulnerability scanning tools you use are regularly updated with all relevant important security vulnerabilities.	
(e)	Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe. Patches should be applied to all systems, even systems that are properly air gapped.	
(f)	Monitor logs associated with any scanning activity and associated administrator accounts to ensure that this activity is limited to the timeframes of legitimate scans.	
(g)	Compare the results from back-to-back vulnerability scans to verify that vulnerabilities were addressed either by patching, implementing a compensating control, or documenting and accepting a reasonable business risk. Such acceptance of business risks for existing vulnerabilities should be periodically reviewed to determine if newer compensating controls or subsequent patches can address vulnerabilities that were previously accepted, or if conditions have changed, increasing the risk.	
(j)	Establish a process to risk-rate vulnerabilities based on the exploitability and potential impact of the vulnerability, and segmented by appropriate groups of assets (example, DMZ servers, internal network servers, desktops, laptops). Apply patches for the riskiest vulnerabilities first. A phased rollout can be used to minimize the impact to the organization. Establish expected patching timelines based on the risk rating level.	

5	**Controlled Use of Administrative Privileges**	
(a)	Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.	To be demonstrated by vendor & checked by BOO
(b)	Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized .	
(c)	Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts.	
(d)	Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators' group, or when a new local administrator account is added on a system.	
(e)	Configure systems to issue a log entry and alert on any unsuccessful login to an administrative account.	
(f)	Use multifactor authentication for all administrative access, including domain administrative access. Multi-factor authentication can include a variety of techniques, to include the use of smart cards,certificates, One Time Password (OTP) tokens, biometrics, or other similar authentication methods.	
(g)	Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).	
(h)	Administrators should be required to access a system using a fully logged and non-administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems.	
(j)	Administrators shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.	
6	**Maintenance, Monitoring, and Analysis of Audit Logs**	
(a)	Include at least two synchronized time sources from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.	To be demonstrated by vendor & checked by BOO
(b)	Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.	
(c)	Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.	
(d)	Have security personnel and/or system administrators run biweekly reports that identify anomalies in logs. They should then actively review the anomalies, documenting their findings.	
(e)	Configure network boundary devices, including firewalls, network-based IPS, and inbound and outbound proxies, to verbosely log all traffic (both allowed and blocked) arriving at the device.	
7	**Email and Web Browser Protections**	
(a)	Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers provided by the vendor in order to take advantage of the latest security functions and fixes.	To be demonstrated by vendor & checked by BOO
(b)	Uninstall or disable any unnecessary or unauthorized browser or email client plugins or add-on applications. Each plugin shall utilize application / URL whitelisting and only allow the use of the application for pre-approved domains.	
(c)	Limit the use of unnecessary scripting languages in all web browsers and email clients. This includes the use of languages such as ActiveX and JavaScript on systems where it is unnecessary to support such capabilities.	
(d)	Log all URL requests from each of the organization's systems, whether onsite or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.	
(e)	Deploy two separate browser configurations to each system. One configuration should disable the use of all plugins, unnecessary scripting languages, and generally be configured with limited functionality and be used for general web browsing. The other configuration shall allow for more browser functionality but should only be used to access specific websites that require the use of such functionality.	

(f)	The organization shall maintain and enforce network based URL filters that limit a system's ability to connect to websites not approved by the organization. The organization shall subscribe to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.	To be demonstrated by vendor & checked by BOO
(g)	To lower the chance of spoofed e-mail messages, implement the Sender Policy Framework (SPF) by deploying SPF records in DNS and enabling receiver-side verification in mail servers.	
(j)	Scan and block all e-mail attachments entering the organization's e-mail gateway if they contain malicious code or file types that are unnecessary for the organization's business. This scanning should be done before the e-mail is placed in the user's inbox. This includes e-mail content filtering and web content filtering.	
8	**Limitation and Control of Network Ports**	
(a)	Ensure that only ports, protocols, and services with validated business needs are running on each system.	To be demonstrated by vendor & checked by BOO
(b)	Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	
(c)	Perform automated port scans on a regular basis against all key servers and compared to a known effective baseline. If a change that is not listed on the organization's approved baseline is discovered, an alert should be generated and reviewed.	
(d)	Verify any server that is visible from the Internet or an untrusted network, and if it is not required for business purposes, move it to an internal VLAN and give it a private address.	
(e)	Operate critical services on separate physical or logical host machines, such as DNS, file, mail, web, and database servers.	
(f)	Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized services or traffic should be blocked and an alert generated.	
9	**Secure Configurations for Network Devices**	
(a)	Compare firewall, router, and switch configuration against standard secure configurations defined for each type of network device in use in the organization. The security configuration of such devices should be documented, reviewed, and approved by an organization change control board. Any deviations from the standard configuration or updates to the standard configuration should be documented and approved in a change control system.	To be demonstrated by vendor & checked by BOO
(b)	All new configuration rules beyond a baseline-hardened configuration that allow traffic to flow through network security devices, such as firewalls and network-based IPS, should be documented and recorded in a configuration management system, with a specific business reason for each change, a specific individual's name responsible for that business need, and an expected duration of the need.	
(c)	Use automated tools to verify standard device configurations and detect changes. All alterations to such files should be logged and automatically reported to security personnel.	
(d)	Manage network devices using two-factor authentication and encrypted sessions.	
(e)	Install the latest stable version of any security-related updates on all network devices.	
(f)	Network engineers shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.	
(g)	Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.	
10	**Boundary Defense**	
(a)	Deny communications with (or limit data flow to) known malicious IP addresses (black lists), or limit access only to trusted sites (whitelists). Tests can be periodically carried out by sending packets from bogon source IP addresses (non-routable or otherwise unused IP addresses) into the network to verify that they are not transmitted through network perimeters. Lists of bogon addresses are publicly available on the Internet from various sources, and indicate a series of IP addresses that should not be used for legitimate traffic traversing the Internet.	To be demonstrated by vendor & checked by BOO
(b)	On DMZ networks, configure monitoring systems (which may be built in to the IDS sensors or deployed as a separate technology) to record at least packet header information, and preferably full packet header and payloads of the traffic destined for or passing through the network border. This traffic should be sent to a properly configured Security Information Event Management (SIEM) or log analytics system so that events can be correlated from all devices on the network.	
(c)	Deploy network-based IDS sensors on Internet and extranet DMZ systems and networks that look for unusual attack mechanisms and detect compromise of these systems. These network-based IDS sensors may detect attacks through the use of signatures, network behavior analysis, or other mechanisms to analyze traffic.	

(d)	Network-based IPS devices should be deployed to complement IDS by blocking known bad signatures or the behavior of potential attacks. As attacks become automated, methods such as IDS typically delay the amount of time it takes for someone to react to an attack. A properly configured network-based IPS can provide automation to block bad traffic. When evaluating network-based IPS products, include those using techniques other than signature-based detection (such as virtual machine or sandbox-based approaches) for consideration.	To be demonstrated by vendor & checked by BOO
(e)	Design and implement network perimeters so that all outgoing network traffic to the Internet must pass through at least one application layer filtering proxy server. The proxy should support decrypting network traffic, logging individual TCP sessions, blocking specific URLs, domain names, and IP addresses to implement a black list, and applying white lists of allowed sites that can be accessed through the proxy while blocking all other sites. Organizations should force outbound traffic to the Internet through an authenticated proxy server on the enterprise perimeter.	
(f)	Require all remote login access (including VPN, dial-up, and other forms of access that allow login to internal systems) to use two-factor authentication.	
(g)	All enterprise devices remotely logging into the internal network should be managed by the enterprise, with remote control of their configuration, installed software, and patch levels. For third-party devices (e.g., subcontractors/vendors), publish minimum security standards for access to the enterprise network and perform a security scan before allowing access.	
(h)	Periodically scan for back-channel connections to the Internet that bypass the DMZ, including unauthorized VPN connections and dual-homed hosts connected to the enterprise network and to other networks via wireless, dial-up modems, or other mechanisms.	
(j)	Deploy NetFlow collection and analysis to DMZ network flows to detect anomalous activity.	
(k)	To help identify covert channels exhilarating data through a firewall, configure the built-in firewall session tracking mechanisms included in many commercial firewalls to identify TCP sessions that last an unusually long time for the given organization and firewall device, alerting personnel about the source and destination addresses associated with these long sessions.	
11	**Controlled Access Based on the Need to Know**	
(a)	Segment the network based on the label or classification level of the information stored on the servers. Locate all sensitive information on separated VLANS with firewall filtering to ensure that only authorized individuals are only able to communicate with systems necessary to fulfill their specific responsibilities.	To be demonstrated by vendor & checked by BOO
(b)	All communication of sensitive information over less-trusted networks should be encrypted. Whenever information flows over a network with a lower trust level, the information should be encrypted.	
(c)	All network switches will enable Private Virtual Local Area Networks (VLANs) for segmented workstation networks to limit the ability of devices on a network to directly communicate with other devices on the subnet and limit an attackers ability to laterally move to compromise neighboring systems.	
(d)	All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principal that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	
(e)	Sensitive information stored on systems shall be encrypted at rest and require a secondary authentication mechanism, not integrated into the operating system, in order to access the information.	
(f)	Enforce detailed audit logging for access to nonpublic data and special authentication for sensitive data.	
(g)	Archived data sets or systems not regularly accessed by the organization shall be removed from the organization's network. These systems shall only be used as stand alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.	
12	**Account Monitoring and Control**	
(a)	Review all system accounts and disable any account that cannot be associated with a business process and owner.	To be demonstrated by vendor & checked by BOO
(b)	Ensure that all accounts have an expiration date that is monitored and enforced.	
(c)	Establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor. Disabling instead of deleting accounts allows preservation of audit trails.	
(d)	Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.	
(e)	Configure screen locks on systems to limit access to unattended workstations.	
(f)	Monitor account usage to determine dormant accounts, notifying the user or user's manager. Disable such accounts if not needed, or document and monitor exceptions (e.g., vendor maintenance accounts needed for system recovery or continuity operations). Require that managers match active employees and contractors with each	

	account belonging to their managed staff. Security or system administrators should then disable accounts that are not assigned to valid workforce members.	
(g)	Use and configure account lockouts such that after a set number of failed login attempts the account is locked for a standard period of time.	To be demonstrated by vendor & checked by BOO
(h)	Monitor attempts to access deactivated accounts through audit logging.	
(j)	Configure access for all accounts through a centralized point of authentication, for example Active Directory or LDAP. Configure network and security devices for centralized authentication as well.	
(k)	Profile each user's typical account usage by determining normal time-of-day access and access duration. Reports should be generated that indicate users who have logged in during unusual hours or have exceeded their normal login duration. This includes flagging the use of the user's credentials from a computer other than computers on which the user generally works.	
(l)	Require multi-factor authentication for all user accounts that have access to sensitive data or systems. Multi-factor authentication can be achieved using smart cards, certificates, One Time Password (OTP) tokens.	
(m)	Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).	
(n)	Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.	
(o)	Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.	
13	**Security Skills Assessment and Appropriate Training to Fill Gaps**	
(a)	Perform gap analysis to see which skills employees need and which behaviors employees are not adhering to, using this information to build a baseline training and awareness roadmap for all employees.	To be demonstrated by vendor & checked by BOO
(b)	Deliver training to fill the skills gap. If possible, use more senior staff to deliver the training. A second option is to have outside teachers provide training onsite so the examples used will be directly relevant. If you have small numbers of people to train, use training conferences or online training to fill the gaps.	
(c)	Implement an security awareness program that (1) focuses only on the methods commonly used in intrusions that can be blocked through individual action, (2) is delivered in short online modules convenient for employees (3) is updated frequently (at least annually) to represent the latest attack techniques, (4) is mandated for completion by all employees at least annually, and (5) is reliably monitored for employee completion.	
(d)	Validate and improve awareness levels through periodic tests to see whether employees will click on a link from suspicious e-mail or provide sensitive information on the telephone without following appropriate procedures for authenticating a caller; targeted training should be provided to those who fall victim to the exercise.	
(e)	Use security skills assessments for each of the mission-critical roles to identify skills gaps. Use hands-on, real-world examples to measure mastery. If you do not have such assessments, use one of the available online competitions that simulate real-world scenarios for each of the identified jobs in order to measure skills mastery.	
14	**Application Software Security**	
(a)	For all acquired application software, check that the version you are using is still supported by the vendor. If not, update to the most current version and install all relevant patches and vendor security recommendations.	To be demonstrated by vendor & checked by BOO
(b)	Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks, including but not limited to cross-site scripting, SQL injection, command injection, and directory traversal attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.	
(c)	For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.	
(d)	Test in-house-developed and third-party-procured web applications for common security weaknesses using automated remote web application scanners prior to deployment, whenever updates are made to the application, and on a regular recurring basis. In particular, input validation and output encoding routines of application software should be reviewed and tested.	
(e)	Do not display system error messages to end-users (output sanitization).	
(f)	Maintain separate environments for production and nonproduction systems. Developers should not typically have unmonitored access to production environments.	
(g)	For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.	

(h)	Ensure that all software development personnel receive training in writing secure code for their specific development environment.	To be demonstrated by vendor & checked by BOO
(j)	For in-house developed applications, ensure that development artifacts (sample data and scripts; unused libraries, components, debug code; or tools) are not included in the deployed software, or accessible in the production environment.	
15	**Incident Response and Management**	
(a)	Ensure that there are written incident response procedures that include a definition of personnel roles for handling incidents. The procedures should define the phases of incident handling.	To be demonstrated by vendor & checked by BOO
(b)	Assign job titles and duties for handling computer and network incidents to specific individuals.	
(c)	Define management personnel who will support the incident handling process by acting in key decision-making roles.	
(d)	Devise organization-wide standards for the time required for system administrators and other personnel to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification. This reporting should also include notifying the appropriate Community Emergency Response Team in accordance with all legal or regulatory requirements for involving that organization in computer incidents.	
(e)	Assemble and maintain information on third-party contact information to be used to report a security incident (e.g., maintain an e-mail address of security@organization.com or have a web page http://organization.com/security).	
(f)	Publish information for all personnel, including employees and contractors, regarding reporting computer anomalies and incidents to the incident handling team. Such information should be included in routine employee awareness activities.	
(g)	Conduct periodic incident scenario sessions for personnel associated with the incident handling team to ensure that they understand current threats and risks, as well as their responsibilities in supporting the incident handling team.	
16	**Penetration Tests and Red Team Exercises**	
(a)	Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully. Penetration testing should occur from outside the network perimeter (i.e., the Internet or wireless frequencies around an organization) as well as from within its boundaries (i.e., on the internal network) to simulate both outsider and insider attacks.	To be demonstrated by vendor & checked by BOO
(b)	Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over.	
(c)	Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.	
(d)	Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, e-mails or documents containing passwords or other information critical to system operation.	
(e)	Plan clear goals of the penetration test itself with blended attacks in mind, identifying the goal machine or target asset. Many APT-style attacks deploy multiple vectors—often social engineering combined with web or network exploitation. Red Team manual or automated testing that captures pivoted and multi-vector attacks offers a more realistic assessment of security posture and risk to critical assets.	
(f)	Use vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts.	
(g)	Wherever possible, ensure that Red Teams results are documented using open, machine-readable standards (e.g., SCAP). Devise a scoring method for determining the results of Red Team exercises so that results can be compared over time.	
(h)	Create a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.	

DRAFT TDs FOR CYBER SECURITY MONITORING CENTRE

1. BLADE ENCLOSURE

Ser No.	Item	Description of Requirement	Compliance
1.	Blade Chassis	Solution to house the required number of blade servers in smallest number of enclosures. Industry standard suitable for housing in Standard Server Racks - The blade enclosure should offer at least 50% more higher server density per square-foot when compared to the dense 1U Rack servers. Should have support for full height and half height blades in the same enclosure, occupying a max of 10U rack height	To be physically checked by BOO
		Same enclosure should support Intel Xeon and EPIC processors based blades	Cert of compliance from Vendor
		Should support Hot Pluggable & Redundant Management Modules with onboard KVM functionality .	
		Should provide an highly reliable and high performance mid-plane/back-plane design in the blade enclosure. Should provide detailed technical information.	
		Should be able to accommodate the blade servers of specifications mentioned in the proposed blade enclosures. The proposals must offer the most dense packaging possible for the blade servers in the enclosure and maximum headroom for future expansion in the offered enclosures.	To be physically checked by BOO
		Support simultaneous remote access for different servers in the enclosure.	To be demonstrated by vendor & checked by BOO
2.	Interconnect	Should support simultaneous housing of FCoE, Ethernet, FC, SAS and infiniband interconnect fabrics offering Hot Pluggable & Redundancy as a feature	To be physically checked by BOO
3.	Blade Server Interconnect to LAN/ Network	The enclosure should support network switches with atleast 2 gigabit uplink ports , up-linkable to the data center switch.	
4.	Blade Server Interconnect to Fiber Channel SAN	The enclosure should support Fiber Channel SAN switches with at least 8 Gb auto-negotiating FC uplinks and also atleast 8Gb auto-negotiating downlinks to all server bays.	Cert of compliance from Vendor
5.	Power Supply	The enclosure should be populated fully with power supplies of the highest capacity available with the vendor. Power supplies should support N+N as well as N+1 redundancy configuration, where N is greater than 1. Should offer a single phase power subsystem enabled with technologies for lower power consumption and offering high energy efficiency levels . Vendors should provide documents certifying the claims.	
6.	Cooling	Each blade enclosure should have a cooling subsystem consisting of redundant hot pluggable fans or blowers enabled with technologies for improved power consumption and acoustics	
7.	System Software	Management/controlling softwares have to be from the OEM.	

Legend. BOO - Board of Officers

8.	Remote Management	Must provide a remote management functionality to operate the server in both in-band and out-of-band. Must be part of the server without the need to install any additional hardware or software.	To be physically checked by BOO
		Must have a real time Virtual KVM functionality and be able to perform a remote Power sequence. Must provide both Java & Java-free browsing options.	
		Must have the ability to map the remote media to the server and ability to transfer files from the user's desktop/laptop folders to the remote server with only the network connectivity.	To be physically checked by BOO
		Must have the ability to capture the video sequence of the last failure and the boot sequence and also playback the video capture or equivalent technology.	
		Must have the ability for multiple administrators across remote locations to collaborate on the remote session in a server with multiple sessions even in server powered OFF mode.	
9.	Power Management	Must be able to show the actual power usage and actual thermal measurement data of the servers.	
10.	Compliance	Vendors must submit supporting documents stating RoHS compliance.	Cert of compliance from Vendor

2. **BLADE SERVER**

SL NO	Item	Description of Requirement	Compliance
1.	CPU	Two numbers of latest generation Intel® Xeon-Gold 6128 (3.4GHz/6-core) processors	To be physically checked by BOO
2.	CPU L3 CACHE Memory	8.25 MB L3 cache to 35.75 MB L3 Cache depending upon processor model chosen	
3.	Motherboard	Intel® C621 Series Chipset	
4.	Memory	16DIMM slots. 64 GB DIMMS scalable upto 1.0 TB using DDR4 Load Reduced DIMM (LRDIMM) operating at 2600 MHz (depending on processor model)	
5.	Memory Protection	Advanced ECC with multi-bit error protection, Online spare, mirrored memory and fast fault tolerance	
6.	Hard disk drive with carrier	2 * 300 GB hot plug SFF SAS/SSD/SATA drives. The drive should have intuitive icon based display along with "DO NOT REMOVE" caution indicator that gets activated automatically in order to avoid data loss/downtime due to wrong drive removal.	
7.	Storage Controller	Server should support Onboard SATA software RAID controller supporting SSD/HDD and at least M.2 drives or 12Gb/s SAS Raid Controller with RAID 0/1/1+0 with 1GB Flash Backed Write Cache	
8.	Networking features	Flexibility to choose one of below embedded ports: 1. Dual Port 20GbE Converged Network Adaptor which supports partitioning up to 7* Ethernet and 1* FC/iSCSI HBA ports per 20Gbps port 2. Dual port 10GbE Converged Network Adaptor which supports partitioning up to 3* Ethernet and 1* FC/iSCSI HBA ports per 10Gbps port 3. Dual port 10Gbps network port which supports partitioning up to 4* Ethernet ports per 10Gbps port 4. Dual port 10Gbps ethernet ports	
9.	Interfaces	Minimum of 1 * internal USB 3.0 port and 1* internal SDHC card slot	
10.	Blade Server Connectivity to SAN	Should be capable of supporting 16 Gbps Dual port Fiber Channel HBA internal to the Server Blade.	

11.	Bus Slots	Minimum of 2Nos of 3.0 PCIe x16 based mezzanine slots supporting Converged Ethernet, Ethernet, FC adapters, SAS and IB adaptors	To be physically checked by BOO
12.	Industry Standard Compliance	ACPI 6.1 Compliant PCIe 3.0 Compliant WOL Support Microsoft® Logo certifications PXE Support USB 3.0 Compliant SMBIOS 3.1 UEFI 2.6 Redfish API	Cert of compliance from Vendor
13.	Embedded system management	Should support monitoring ongoing management, service alerting, reporting and remote management with embedded Gigabit out of band management port Server should support configuring and booting securely with industry standard Unified Extensible Firmware System should support RESTful API integration System management should support provisioning servers by discovering and deploying 1 to few servers with Intelligent Provisioning System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support	To be demonstrated by vendor & checked by BOO
14.	Security	UEFI Secure Boot and Secure Start support Security feature to ensure servers do not execute compromised firmware code Support for Commercial National Security Algorithms (CNSA) Granular control over remote management interfaces Tamper-free updates - components digitally signed and verified Secure Recovery - recover critical firmware to known good state on detection of compromised firmware TPM (Trusted Platform Module) 1.2 option TPM (Trusted Platform Module) 2.0 option Bezel Locking Kit	Cert of compliance from Vendor
15.	OS Support	Microsoft Windows Server VMware Red Hat Enterprise Linux Server SUSE Linux Enterprise Server	To be physically checked by BOO
16.	Secure encryption	System should support Encryption of the data on both the internal storage and cache module of the array controllers using encryption keys. Should support local key management for single server and remote key management for central management for enterprise-wide data encryption deployment.	Cert of compliance from Govt Auth Lab/OEM
17.	Provisioning	Essential tools, drivers, agents to setup, deploy and maintain (not the OS) the server should be embedded inside the server. There should be a built -in update manager that can update these tools online.	To be physically checked by BOO
18.	Firmware security	1. For firmware security, system should support remote management chip creating a fingerprint in the silicon, preventing servers from booting up unless the firmware matches the fingerprint. This feature should be immutable 2. Should maintain repository for firmware and drivers recipes to aid rollback or patching of compromised firmware. Should also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware	Cert of compliance from Vendor

19.	Embedded Remote Management and firmware security	1. System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder; It should support server power capping and historical reporting and should have support for multifactor authentication 2. Server should have dedicated remote management port 3. Remote management port should have storage space earmarked to be used as a repository for firmware, drivers and software components. The components can be organized in to install sets and can be used to rollback/patch faulty firmware 3. Server should support agent less management using the out-of-band remote management port 4. The server should support monitoring and recording changes in the server hardware and system configuration. It assists in diagnosing problems and delivering rapid resolution when system failures occur 5. Applications to access the server remotely using popular handheld devices based on Android or Apple IOS should be available 6. Remote console sharing upto 6 users simultaneously during pre-OS and OS runtime operation, Console replay - Console Replay captures and stores for replay the console video during a server's last major fault or boot sequence. Microsoft Terminal Services Integration, 128 bit SSL encryption and Secure Shell Version 2 support. Should provide support for AES and 3DES on browser. Should provide remote firmware update functionality. Should provide support for Java free graphical remote console. 7. Should support managing multiple servers as one via Group Power Control Group Power Capping Group Firmware Update Group Configuration Group Virtual Media Group License Activation 8. Should support RESTful API integration 9. System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support	To be demonstrated by vendor & checked by BOO
20.	Server Management	Software should support dashboard view to quickly scan the managed resources to assess the overall health of the data center. It should provide an at-a-glance visual health summary of the resources user is authorized to view.	To be physically checked by BOO
		The Dashboard minimum should display a health summary of the following: • Server Profiles • Server Hardware • Enclosures • Logical Interconnects • Appliance alerts	
		The Systems Management software should provide Role-based security	To be demonstrated

		Software should support search for resource-specific information such as specific instances of resource names, serial numbers, WWNs, IP and MAC addresses to help manage infrastructure better	by vendor & checked by BOO
		Management software should support integration with popular virtualization platform management software like vCenter, SCVMM and RedHat RHEV	
		Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD.	
		Should provide an online portal that can be accessible from anywhere. The portal should provide one stop, online access to the product, support information and provide information to track warranties, support contracts and status. The Portal should also provide a Personalised daskboard to monitor device heath, hardware events, contract and warranty status. Should provide a visual status of individual devices and device groups. The Portal should be available on premise (at our location - console based) or off premise (in the cloud).	
		Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components.	
		The Server Management Software should be of the same brand as of the server supplier.	To be physically checked by BOO

3. STORAGE SERVER

Ser No	Item	Description	Compliance
Compute Nodes chassis Specifications			
1	Chassis	Vendor should offer a Server chassis / enclosure based solution which can hold dense servers(Compute nodes with pure CPUs only) on an average of 0.5U per Server, capable of getting mounted in a standard 19" 42U Rack (max depth of 1200mm). 0.5U average form factor is at the Enclosure / Chassis level only. Each of the Server nodes should be individually serviceable, without shutting down the other Server nodes.	To be physically checked by BOO
2	Cooling	The chassis / enclosure should be configured with redundant fans. The fans should be serviceable without shutting down the Enclosure / Chassis.	
3	Redundant Power Supplies	The entire solution should be offered with redundant power supplies either at Rack level or enclosure level. N+1 redundancy to be configured.	
4	Management	Chassis Controller with integrated management port, regulates chassis supplies, fans, compute nodes and switches; Advanced thermal technology to minimize power consumption and reduce cooling when nodes not fully utilized.	
5	Networking	The chassis should be capable of supporting the following type of Interconnects: (a) Infiniband EDR (single rail) (b) Intel Omnipath Architecture (OPA) - single rail and dual rail options (c) Combination of EDR and OPA within the chassis (d) 2x Integrated Ethernet with 10G downlinks and 10G/40G uplinks OR 10G Pass-Through Module w/6 QSFP+ ports(breakout to 24 10G ports) (e) Future support for EDR/HDR IB switch	To be demonstrated by vendor & checked by BOO
Compute Node Specifications:- Each of the compute nodes in the chassis/enclosure should be configured with the following:			

1	CPU	Two nos of Intel® Xeon-Gold 6144 (3.5GHz/8-core) (Skylake) processors	To be physically checked by BOO
3	Memory Requirement	16DIMM slots should be available. 128GB DIMMS scalable upto 1024 GB using DDR4 Load Reduced DIMM (LRDIMM) operating at 2666 MT/s	
5	Memory protection	Advanced ECC , Memory Online Spare Mode, Memory Mirroring Mode	To be demonstrated by vendor & checked by BOO
6	Disks scalability	2 nos 600GB SAS HDD and saleable Upto 4 nos of hard drive bays	To be physically checked by BOO
7	Infiniband	Should support upto '2 x EDR/OPA HCAs'	Cert of compliance from Vendor
8	Networking	Integrated 2 x 1Gb/10Gb ethernet ports	To be physically checked by BOO
9	Management Port	1Gbps Management Port - at Enclosure level	
10	PCI-Express 3.0 slots	The compute node should have atleast 1 no. of PCIe - Gen3 (x8) low profile slot for adding internal devices like Hardware RAID controller.	
11	Operating Systems and Virtualization Software Support	Microsoft Windows Server Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) Vmware CentOS	
12	System tuning for performance	1. System should support feature for improved workload throughput for applications sensitive to frequency fluctuations. This feature should allow processor operations in turbo mode without the frequency fluctuations associated with running in turbo mode 2. System should support workload Profiles for simple performance optimization	Cert of compliance from Vendor
13	Secure encryption	System should support Encryption of the data (Data at rest) on both the internal storage and cache module of the array controllers using encryption keys. Should support local key management for single server and remote key management for central management for enterprise-wide data encryption deployment.	Cert of compliance from Govt Auth Lab/OEM
14	Provisioning	1. Should support tool to provision server using REST ful API to discover and deploy servers at scale 2, Provision one to many servers using own scripts to discover and deploy with Scripting Tool (STK) for Windows and Linux or Scripting Tools for Windows Power Shell	Cert of compliance from Vendor
15	Firmware security	1. For firmware security, system should support remote management chip creating a fingerprint in the silicon, preventing servers from booting up unless the firmware matches the fingerprint. This feature should be immutable 2. Should maintain repository for firmware and drivers recipes to aid rollback or patching of compromised firmware. Should also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware	

4. RACK SERVER

Ser No	Item	Description of Requirement	Compliance
1.	CPU	Two numbers of latest generation Intel® Xeon-Gold 6134 (3.2GHz/8-core) processors	To be physically

2.	CPU L3 CACHE Memory	8.25 MB L3 cache to 38.5 MB L3 cache depending upon processor model chosen	checked by BOO
3.	Motherboard	Intel® C621 Series Chipset	
4.	Memory	24DIMM slots. 128GB DIMMS scalable upto 1.5 TB using DDR4 Load Reduced DIMM (LRDIMM) operating at 2600 MHz (depending on processor model)	
5.	Memory Protection	Advanced ECC with multi-bit error protection, Online spare, mirrored memory and fast fault tolerance	To be demonstrated by vendor & checked by BOO
6.	HDD Bays	Up to 8+2 SFF HDD/SSD or 10 NVMe PCIe SSD. The drive carrier should have intutiveicon based display along with "DO NOT REMOVE" caution indicator that gets activated automatically in order to avoid data loss/downtime due to wrong drive removal.	To be physically checked by BOO
7.	Hard disk drive	2 Nos 600GB 10K RPM 12G HDD	
8.	Controller	Server should support Onboard SATA software RAID controller supporting SSD/HDD and at least two M.2 drives. In addition, server should support one of the below controllers supporting Mixed Mode which combines RAID and HBA mode, PCIe 3.0 based 12Gb/s SAS Raid Controller with RAID 0/1/1+0/5/50/6/60/1 Advanced Data Mirroring/10 Advanced Data Mirroring (onboard or on a PCI Express slot) or PCIe 3.0 based 12Gb/s SAS Raid Controller with RAID 0/1/1+0/5/50/6/60/1 Advanced Data Mirroring/10 Advanced Data Mirroring with 4GB battery backed write cache (onboard or on a PCI Express slot) Storage controller should support Secure encryption/data at rest Encryption	To be demonstrated by vendor & checked by BOO
9.	Networking features	Server should support below networking cards: 1. 1Gb 4-port network adaptors 2. 10Gb 2-port Ethernet adaptor 3. 10GBaseT 4-port Ethernet adaptor 4. 4x25Gb Ethernet adaptor 5. 10/25Gb 2-port Ethernt adaptor Infiniband Options: 40Gb dual port or 100Gb Single or Dual port Adapter 100Gb Single port Omni path adaptor	To be physically checked by BOO
10.	Interfaces	Serial - 1 Micro SD slot - 1 USB 3.0 support With Up to 5 total: 1 front, 2 internal, 2 rear, 2 internal (secure)	
11.	Bus Slots	Three PCI-Express 3.0 slots, atleast two x16 PCIe slots	
12.	Power Supply	Should support hot plug redundant low halogen power supplies with minimum 94% efficiency	
13.	Fans	Redundant hot-plug system fans	
14.	Industry Standard Compliance	ACPI 6.1 Compliant PCIe 3.0 Compliant PXE Support WOL Support Microsoft® Logo certifications USB 3.0 Support USB 2.0 Support Energy Star	Cert of compliance from Vendor

		ASHRAE A3/A4 UEFI (Unified Extensible Firmware Interface Forum) SMBIOS Redfish API IPMI 2.0 SNMP v3 TLS 1.2 DMTF Systems Management Architecture Active Directory v1.0	
15.	System Security	UEFI Secure Boot and Secure Start support Security feature to ensure servers do not execute compromised firmware code FIPS 140-2 validation Common Criteria certification Configurable for PCI DSS compliance Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser Support for Commercial National Security Algorithms (CNSA) mode to prevent the use of insecure algorithms Tamper-free updates - components digitally signed and verified Secure Recovery - recover critical firmware to known good state on detection of compromised firmware. Ability to rollback firmware Secure erase of NAND/User data TPM (Trusted Platform Module) 1.2 TPM (Trusted Platform Module) 2.0 Bezel Locking Kit option Chassis Intrusion detection option Support for Commercial National Security Algorithms (CNSA) Smart card (PIV/CAC) and Kerberos based 2-factor Authentication. Configurable for PCI DSS compliance. Secure erase of NAND	Cert of compliance from Vendor
16.	Operating Systems and Virtualization Software Support	Microsoft Windows Server Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) VMware ClearOS	To be physically checked by BOO
17.	GPU support	System should support NVIDIA's latest computational accelerators and graphics accelerators	Cert of compliance from Vendor
18.	System tuning for performance	1. System should support feature for improved workload throughput for applications sensitive to frequency fluctuations. This feature should allow processor operations in turbo mode without the frequency fluctuations associated with running in turbo mode 2. System should support workload Profiles for simple performance optimization	To be demonstrated by vendor & checked by BOO
19.	Secure encryption	System should support Encryption of the data (Data at rest) on both the internal storage and cache module of the array controllers using encryption keys. Should support local key management for single server and remote key management for central management for enterprise-wide data encryption deployment.	Cert of compliance from Govt Auth Lab/OEM
20.	Provisioning	1. Should support tool to provision server using RESTful API to discover and deploy servers at scale 2, Provision one to many servers using own scripts to discover and deploy with Scripting Tool (STK) for Windows and Linux or Scripting Tools for Windows Power Shell	Cert of compliance from Vendor

21.	Firmware security	1. For firmware security, system should support remote management chip creating a fingerprint in the silicon, preventing servers from booting up unless the firmware matches the fingerprint. This feature should be immutable 2. Should maintain repository for firmware and drivers recipes to aid rollback or patching of compromised firmware. Should also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware	
22.	Embedded Remote Management and firmware security	1. System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder; It should support server power capping and historical reporting and should have support for multifactor authentication 2. Server should have dedicated 1Gbps remote management port 3. Remote management port should have storage space earmarked to be used as a repository for firmware, drivers and software components. The components can be organized in to install sets and can be used to rollback/patch faulty firmware 3. Server should support agentless management using the out-of-band remote management port 4. The server should support monitoring and recording changes in the server hardware and system configuration. It assists in diagnosing problems and delivering rapid resolution when system failures occur 5. Applications to access the server remotely using popular handheld devices based on Android or Apple IOS should be available 6. Remote console sharing upto 6 users simultaneously during pre-OS and OS runtime operation, Console replay - Console Replay captures and stores for replay the console video during a server's last major fault or boot sequence. Microsoft Terminal Services Integration, 128 bit SSL encryption and Secure Shell Version 2 support. Should provide support for AES and 3DES on browser. Should provide remote firmware update functionality. Should provide support for Java free graphical remote console. 7. Should support managing multiple servers as one via Group Power Control Group Power Capping Group Firmware Update Group Configuration Group Virtual Media Group License Activation 8. Should support RESTful API integration 9. System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support	To be demonstrated by vendor & checked by BOO

23.	Server Management	Software should support dashboard view to quickly scan the managed resources to assess the overall health of the data center. It should provide an at-a-glance visual health summary of the resources user is authorized to view.	To be physically checked by BOO
		The Dashboard minimum should display a health summary of the following: • Server Profiles • Server Hardware • Appliance alerts	
		The Systems Management software should provide Role-based access control	To be demonstrated by vendor & checked by BOO
		Management software should support integration with popular virtualization platform management software like vCenter, and SCVMM	
		Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD.	
		Should provide an online portal that can be accessible from anywhere. The portal should provide one stop, online access to the product, support information and provide information to track warranties, support contracts and status. The Portal should also provide a Personalised dashboard to monitor device heath, hardware events, contract and warranty status. Should provide a visual status of individual devices and device groups. The Portal should be available on premise (at our location - console based) or off premise (in the cloud).	
		Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components.	To be demonstrated by vendor & checked by BOO
		The Server Management Software should be of the same brand as of the server supplier.	To be physically checked by BOO

5. UNIFIED THREAD MANAGEMENT

Ser No	Description of Requirements	Compliance
General Requirements		
1	Network security appliance should support "Stateful" policy inspection technology. It should also have application intelligence for commonly used TCP/IP protocols like telnet, ftp etc.	To be demonstrated by vendor & checked by BOO
2	The proposed vendor must have a track record of continuous improvement in threat detection (IPS) and must have successfully completed NSS Labs' NGFW Methodology v7.0 testing with a minimum exploit blocking rate of 99%	Cert of compliance from Vendor
3	OEM should be in Leaders quadrant of Gartner's – in Enterprise Firewall Magic Quadrant as per the latest report	
4	Appliance shall be ICSA certified for Firewall, IPS, Gateway AntiVirus, IPSec VPN, SSL VPN functionalities	Cert of compliance from Govt Auth Lab/OEM
Hardware & Interface requirements		
1	14 x 1GE RJ45 inbuilt interfaces, 4 x 1GE SFP interface slots from day one	To be physically

2	The Appliance should have 1x USB, 1x dedicated Console Port	checked by BOO
Performance and Availability		
1	The Firewall should be on ASIC Based multiprocessor architecture with minimum 18 Gbps of Firewall throughput for 1518 byte packet size, 2,000,000 concurrent sessions, and 130,000 new sessions per second support from day one and Firewall Latency should not be more than 3µs	To be demonstrated by vendor & checked by BOO
2	Minimum IPS throughput of 5500 Mbps from day one	
3	Proposed solution must support minimum 1 Gbps of SSL Inspection throughput	
4	IPSec VPN throughput: minimum 8 Gbps	
5	Simultaneous IPSec VPN tunnels: 500	
6	Should have 200 SSL VPN peer support from day one	
7	Proposed solution must support minimum 10 virtual firewall from day one	
Routing Protocols		
1	Static Routing	To be demonstrated by vendor & checked by BOO
2	Policy Based Routing	
3	The Firewall should support dynamic routing protocol like RIP, OSPF, BGP, ISIS	
Firewall Features		
1	Firewall should provide application inspection for LDAP, SIP, H.323, SNMP, FTP,SMTP, HTTP, DNS, ICMP, DHCP, RPC,SNMP, IMAP, NFS etc	To be demonstrated by vendor & checked by BOO
2	IPv6-enabled inspection services for applications based on HTTP, FTP, SMTP, ICMP, TCP, and UDP	
3	Allows secure deployment of next-generation IPv6 networks, as well as hybrid environments that require simultaneous, dual stack support of IPv4 and IPv6	
4	The firewall should support transparent (Layer 2) firewall or routed (Layer 3) firewall Operation	
5	The Firewall should support ISP link load balancing.	
6	Firewall should support link aggregation functionality to group multiple ports as single port.	
7	Firewall should support minimum VLANS 2048	
8	Firewall should support static NAT, policy based NAT and PAT	
9	Firewall should support IPSec data encryption	
10	It should support the IPSec VPN for both site-site and remote access VPN	
11	Firewall should support IPSec NAT traversal.	
12	Support for standard access lists and extended access lists to provide supervision and control	
13	control SNMP access through the use of SNMP and MD5 authentication.	
14	Firewall system should support virtual tunnel interfaces to provision route-based IPSec VPN	
15	The Firewall should have integrated solution for SSL VPN	
16	Should support LDAP, RADIUS, Windows AD, PKI based Authentication & should have integrated 2-Factor Authentication server support & this two factor authentication can be used for VPN users for accessing internal network from outside and for Local users accessing internet from inside the network and for administrative access to the appliance or all of them	
17	The solution should have basic server load balancing functionality as an inbuilt feature	
18	Licensing should be a per device and not user or IP based (should support unlimited users)	To be physically checked by BOO
Integrated IPS Features Set		
1	IPS should have DDoS and DoS anomaly detection and protection mechanism with threshold configuration.	
2	Support SYN detection and protection for both targets and IPS devices.	
3	The device shall allow administrators to create Custom IPS signatures	

4	Should have a built-in Signature and Anomaly based IPS engine on the same unit	To be demonstrated by vendor & checked by BOO
5	Signature based detection using real time updated database & should have minimum 10000+ IPS signature database from day one	
6	Supports automatic security updates directly over the internet. (ie no dependency of any intermediate device)	
7	Signature updates do not require reboot of the unit.	
8	Configurable IPS filters to selectively implement signatures based on severity, target (client/server) and operating systems	
9	IPS Actions: Default, monitor, block, reset, or quarantine	
10	Should support packet capture option	
11	IP(s) exemption from specified IPS signatures	
12	Should support IDS sniffer mode	
Anti Virus & Anti Bot		
1	Firewall should support antimalware capabilities , including antivirus, botnet traffic filter and antispyware	To be demonstrated by vendor & checked by BOO
2	Solution should be able to detect and prevent unique communication patterns used by BOTs i.e. information about botnet family	
3	Solution should be able to block traffic between infected host and remote operator and not to legitimate destination	
4	Should have antivirus protection for protocols like HTTP, HTTPS, IMAPS, POP3S, SMTPS protocols etc.	
5	Solution should have an option of packet capture for further analysis of the incident	
6	Solution should uncover threats hidden in SSL links and communications	
7	The AV should scan files that are passing on CIFS protocol	
8	The proposed system shall provide ability to allow, block attachments or downloads according to file extensions and/or file types	
9	The proposed system should be able to block or allow oversize file based on configurable thresholds for each protocol types and per firewall policy.	
Other support		
1	Should support features like Web-Filtering, Application-Control & Gateway level DLP from day one	To be demonstrated by vendor & checked by BOO
2	The proposed system should have integrated Enterprise-class Web Content Filtering solution with database which should support over 250 million webpages in 72+ categories and 68+ languages without external solution, devices or hardware modules.	
3	Should support detection over 3,000+ applications in multiple Categories: Botnet, Collaboration, Email, File Sharing, Game, General Interest, Network Service, P2P, Proxy, Remote Access, Social Media, Storage Backup, Update, Video/Audio, VoIP, Industrial, Special, Web (Others)	
4	The product must supports Layer-7 based UTM/Firewall virtualization, and all UTM features should be supported in each virtual firewall like Threat Prevention, IPS, Web filter, Application Control, content filtering etc.	
5	The solution should have the flexibility to write security policies based on IP Address & User Name & Endpoint Operating System	
6	QoS features like traffic prioritization, differentiated services,. Should support for QoS features for defining the QoS policies.	
7	It should support the VOIP traffic filtering	
8	Appliance should have identity awareness capabilities	
9	The firewall must support Active-Active as well as Active-Passive redundancy.	
10	Solution must support VRRP clustering protocol.	
Management & Reporting functionality		
1	Support for Built-in Management Software for simple, secure remote management of the security appliances through integrated, Web-based	To be demonstrated

	GUI.	by vendor & checked by BOO
2	Support accessible through variety of methods, including console port, Telnet, and SSHv2	
3	Support for both SNMPv2 and SNMPv2c, providing in-depth visibility into the status of appliances.	
4	Should have capability to import configuration and software files for rapid provisioning and deployment using Trivial File Transfer Protocol (TFTP), HTTP, HTTPS	
5	The Firewall appliance should have minimum 450GB of internal storage for local reporting	
6	Solution must allow administrator to choose to login in read only or read-write mode	

6. CENTRAL NETWORK ASSET MANAGER

Ser No	Description of Requirements	Compliance
1	Should be a comprehensive management platform that delivers integrated, modular management capabilities across fault, configuration, accounting, performance, and security (FCAPS) needs	To be demonstrated by vendor & checked by BOO
2	Should support minimum 500 wired devices from day 1 and the solution should be scalable up to 1500 wired devices without any hardware or software up-gradation.	
3	Should allow automatic topology discovery and creation of network maps for layer 2 as well as layer 3 networks including all the available VLANs	
4	Should have network inventory polling capability for IP network nodes, available line cards, modules, ports, physical links, VLAN interfaces and all the other SNMP capable devices in the network.	
5	Should allow extensive fault management with real time event and alarm notifications including system logs	
6	Should allow centralized creation and management of VLAN and ACL policies	
7	Should have scheduled device configuration back-up and restore functionality	
8	Should have automatic detection of configuration changes for easy trouble shooting and isolation.	
9	Should allow monitoring and management of 3rd party devices and end points.	
10	Should have the functionality of scheduled configuration roll out	
11	Should have the functionality to perform scheduled or unscheduled network wide software or firmware upgrades	
12	Should have the ability to customize NMS dash board.	
13	Should allow grouping of devices for applying any particular change/task	
15	Should have 64-bit support	
16	Should support centralized as well as distributed deployment.	
17	Should support virtualization management; management and monitoring of both physical and virtual networks. It should provide insight into and management of virtual networks and reduce migration complexity by aligning and automatic network policies with virtual images.	
18	Should support role based access control	
19	Should be with software update and upgrade assurance during the warranty period	
20	Should have support for add-on modules on the same software platform for monitoring and management of routers, wireless controller, wireless access points and wireless client devices.	
21	Should facilitate enable centralized management of proposed network elements with a variety of automated tasks, including discovery, categorization, baseline	
	configurations, software images, configuration comparison tools, version tracking, change alerts, and more	
22	Should support centralized VLAN Management to view current VLAN configuration, VLAN topology, bulk VLAN deployment etc.	
23	a) Should provide high-performance, scalable network log audit and analysis support with auditing online activities of internal users	Cert of compliance from Vendor
	b) Should support various log formats such as NAT, flow, NetStream	

	including log formats that allows audit security-sensitive operations and digest data from HTTP, FTP, and SMTP packets	
	c) Should support policy driven log filtering	
	d) Should support log collection from devices that do not otherwise support the standard protocols such as Flow, NAT, NetStream, sFlow/Netflow etc.	
	e) Should support user activity auditing of at least 50 users from day 1 and this should be optionally extendable up to 1500 users.	
24	Should offer following RADIUS/AAA features:	
	a) Shall support user identity authentication based on the access policies associated with infrastructure resources, such as routers, switches, license for 100 users from day 1.	To be demonstrated by vendor & checked by BOO
	b) Shall provide a full-featured RADIUS server that supports centralized authentication, authorization, and accounting management.	Cert of compliance from Vendor
	c) Network-agnostic device fingerprinting capabilities based on HTTP+MAC+DHCP device recognition for BYOD.	
	d) Shall support authentication modes like 802.1X, VPN, portal, and wireless access identity modes like PAP, CHAP,EAP-MD5, EAP-TLS, and PEAP to fit into applications with different security requirements.	
	e) Shall provide centralized policy creation to set the appropriate access rights for each type of user and device across the network.	
25	Should be a ITILv3 compliant comprehensive management platform that delivers integrated, modular management capabilities across fault, configuration, accounting, performance, and security (FCAPS) needs.	Cert of compliance from Vendor
26	Offered software should have compatibility with Microsoft Windows or Linux operating systems	To be physically checked by BOO
27	Offered software should be scalable up to 1500 wired devices and 1500 users.	Cert of compliance from Vendor

7. NETWORK ASSET MANAGER

S. No.	Description of Requirements	Compliance
1	Should be a comprehensive management platform that delivers integrated, modular management capabilities across fault, configuration, accounting, performance, and security (FCAPS) needs	To be demonstrated by vendor & checked by BOO
2	Should support minimum 500 wired devices from day 1 and the solution should be scalable up to 1500 wired devices without any hardware or software up-gradation.	
3	Should allow automatic topology discovery and creation of network maps for layer 2 as well as layer 3 networks including all the available VLANs	
4	Should have network inventory polling capability for IP network nodes, available line cards, modules, ports, physical links, VLAN interfaces and all the other SNMP capable devices in the network.	
5	Should allow extensive fault management with real time event and alarm notifications including system logs	
6	Should allow centralized creation and management of VLAN and ACL policies	
7	Should have scheduled device configuration back-up and restore functionality	
8	Should have automatic detection of configuration changes for easy trouble shooting and isolation.	
9	Should allow monitoring and management of 3rd party devices and end points.	
10	Should have the functionality of scheduled configuration roll out	
11	Should have the functionality to perform scheduled or unscheduled network wide software or firmware upgrades	
12	Should have the ability to customize NMS dash board.	
13	Should allow grouping of devices for applying any particular change/task	
15	Should have 64-bit support	

16	*Should support centralized as well as distributed deployment.*	
17	Should support virtualization management; management and monitoring of both physical and virtual networks. It should provide insight into and management of virtual networks and reduce migration complexity by aligning and automatic network policies with virtual images.	
18	Should support role based access control	To be demonstrated by vendor & checked by BOO
19	Should be with software update and upgrade assurance during the warranty period	
20	Should have support for add-on modules on the same software platform for monitoring and management of routers, wireless controller, wireless access points and wireless client devices.	
21	Should facilitate enable centralized management of proposed network elements with a variety of automated tasks, including discovery, categorization, baseline	
	configurations, software images, configuration comparison tools, version tracking, change alerts, and more	
22	Should support centralized VLAN Management to view current VLAN configuration, VLAN topology, bulk VLAN deployment etc.	
23	a) Should provide high-performance, scalable network log audit and analysis support with auditing online activities of internal users	
	b) Should support various log formats such as NAT, flow, NetStream including log formats that allows audit security-sensitive operations and digest data from HTTP, FTP, and SMTP packets	Cert of compliance from Vendor
	c) Should support policy driven log filtering	
	d) Should support log collection from devices that do not otherwise support the standard protocols such as Flow, NAT, NetStream, sFlow/Netflow etc.	
	e) Should support user activity auditing of at least 50 users from day 1 and this should be optionally extendable up to 1500 users.	
24	Should offer following RADIUS/AAA features:	
	a) Shall support user identity authentication based on the access policies associated with infrastructure resources, such as routers, switches, license for 100 users from day 1.	To be demonstrated by vendor & checked by BOO
	b) Shall provide a full-featured RADIUS server that supports centralized authentication, authorization, and accounting management.	
	c) Network-agnostic device fingerprinting capabilities based on HTTP+MAC+DHCP device recognition for BYOD.	Cert of compliance from Vendor
	d) Shall support authentication modes like 802.1X, VPN, portal, and wireless access identity modes like PAP, CHAP,EAP-MD5, EAP-TLS, and PEAP to fit into applications with different security requirements.	
	e) Shall provide centralized policy creation to set the appropriate access rights for each type of user and device across the network.	
25	Should be a ITILv3 compliant comprehensive management platform that delivers integrated, modular management capabilities across fault, configuration, accounting, performance, and security (FCAPS) needs.	Cert of compliance from Vendor
26	Offered software should have compatibility with Microsoft Windows or Linux operating systems	To be physically checked by BOO
27	Offered software should be scalable up to 1500 wired devices and 1500 users.	Cert of compliance from Vendor

8. CENTRAL EVENT & LOG MANAGER

Ser No	Description of Requirements	Compliance
1	The solution should have a separate appliance for storing logs & generating reports centrally for all connected Firewalls of the same OEM & should have minimum capacity of connecting 30 Firewalls	To be physically checked by BOO
2	The proposed centralized logging & reporting solution should have a capacity of accepting minimum 200GB logs per day & a total storage capacity of 12TB.	

3	The solution should have support for RAID 0/1/5/10	Cert of compliance from Vendor
4	The reporting solution should have customizable interactive dashboard to rapidly pinpoint problems	To be physically checked by BOO
5	It should support drill-down to follow the trail of an attacker, trace transactions and gain new insights	To be demonstrated by vendor & checked by BOO
6	It should have minimum 25+ built-in templates with sample reports ready for use	To be physically checked by BOO
7	The solution should support to run report on-demand or on a schedule with automated email notification and Calendar view	To be demonstrated by vendor & checked by BOO
8	It should support customization with 300+ built-in charts ready for generating custom reports	
9	The solution should provide flexible report formats like HTML/CSV/XML/PDF	
10	It should support retrieving of archived logs to perform analytics against historic data	
11	The solution should support forwarding of logs to a Syslog server or a CEF log server for long-term storage, forensics or regulatory compliance	To be demonstrated by vendor & checked by BOO

9. CENTRAL POLICY MANAGER

Ser No	Description of Requirements	Compliance
1	The solution should have a centralized management appliance for managing minimum 30 Firewall appliances of the same OEM from a single console	To be physically checked by BOO
2	The management solution can collectively configure the device settings, objects and policies across the network from a single user interface	
3	The management solution can review, approve and audit policy changes from a central place	Cert of compliance from Vendor
4	It should support automated process to facilitate policy compliance and policy lifecycle management	
5	Should support enforcing workflow to reduce risk for policy changes	
6	The centralized management solution should support for: Application Control and Intrusion. Prevention updates, Vulnerability Management, Antivirus and Web Filtering updates to all the connected Firewall appliances from a single console	To be demonstrated by vendor & checked by BOO
7	It should support for RESTful API which allows to create customized, branded web portals for policy and object administration	Cert of compliance from Vendor
8	Should capable to provide a convenient method for alerting administrators when critical events are encountered, by sending e-mail alert messages to administrator defined e-mail addresses	
9	The solution should support ensuring common security baseline to be enforced and shared among multiple administrative domains (ADOMs).	

10. DATA LEAKAGE ENDPOINT

Ser No	Required Technical Descriptions	Compliance
1	The solution should be able to enforce policies by URL's, domains or support URL categories by integrating with Network DLP .The solution should be able to monitor FTP access and traffic including file access transferred and file data with control information.	To be demonstrated by vendor & checked by BOO
2	The solution should detect and prevent content getting posted or uploaded to specific websites, blogs, and forums accessed over HTTP , HTTPS.	
3	The solution should inspect data leaks over HTTP , HTTPs and SMTP. The solution should be able to inspect HTTP traffic and HTTPs traffic natively . Should provide support both build-in SSL decryption and destination awareness capability with integration with Network and Gateway DLP controls.	

4	The solution should be able to block outbound emails sent via SMTP if its violates the policy. Also natively monitors and block the internal emails shared between the different department.	To be demonstrated by vendor & checked by BOO
5	The solution should have more than 50 pre-defined applications and multiple application groups and allow each application/application group to monitor operations like Cut/Copy, Paste, File Access and Screen Capture or Download. Also solution should have the capability to define the third party application.	
6	The solution should be able to monitor data copied to network file shares and should enforce structured and unstructured fingerprint policies even when disconnected from corporate network.	
7	The endpoint would be able to store both structured and unstructured fingerprints on the endpoint itself and should perform all analysis locally and not contact and network components to reduce WAN overheads. The solution should be able to enforce different policies for desktops and laptops.	
8	The endpoint solution should have capabilities to monitor applications and ensure unauthorized applications do not have access to sensitive files. The endpoint solution should be able to perform discovery only when the endpoint is connected to external power or Machine is Idle.	
9	The solution should Provide “Cloud Storage Applications ” group which monitor sensitive content accessed by these cloud storage application on the endpoint and prevent sensitive data from uploading to the cloud . For Example (Should support from day 1(Windows 10 and MAC OSX 10.11) - Amazon Cloud Drive Box Dropbox Google Drive SkyDrive ICloud)	To be demonstrated by vendor & checked by BOO
10	The endpoint solution should Blocking of non-Windows CD/DVD burners, it should also Inspect and optionally block Explorer writes to WPD class devices. The endpoint solution should encrypt information copied to removable media	
11	Endpoint solution should support win 32 and 64 bit OS, Mac & Linux OS, Support wide variety of platforms(Below support from Day1): • Windows 7 • Windows 8 and 10 • Windows server 2008 • Windows server 2008 R2 • Windows server 2012 • Mac OS X -10.11 , 10.12 and 10.13 • Red Hat Linux/Cent OS , VDI (CItrix and VMWare)	Cert of compliance from Vendor
12	The solution should have a comprehensive list of pre-defined policies and templates with over 1700+ patterns to identify and classify information pertaining to different industry like Energy, Petroleum industry vertical etc and India IT Act. The solution should provide capabilities to identify data based on keywords or dictionaries and the solution should be able to enforce policies based on file types, size of files and also the name of the file	
13	The proposed DLP solution should be able to encrypt content copied to removable media natively and manage the Encryption and DLP policies from the same management Console. Should support both Native and Portable Encryption.	Cert of compliance from Govt Auth Lab/OEM
14	The proposed solution should provide pre-defined policies for identifying possible for identifying possible expression that are indicative of cyber bullying , self destructive pattern or employee discontent , Mail to Self .	Cert of compliance from Vendor
15	The solution should be able to detect encrypted and password protected files. The solution should be able to do full binary fingerprint of files and also should be able to detect even if partial information gets leaks from fingerprinted files or folders. The solution should be able to recursively inspect the content of compressed archives	
16	The solution should be able to fingerprint only specific fields or columns within a database and should be able to identify information from databases by correlating information residing in different columns in a database	

17	The Solution should have advanced Machine Learning – Ability to automatically learn sensitive information from copies of information that needs to be protected and also automatically learn false positives.	
18	The solution should enforce policies to detect low and slow data leaks.	
19	The solution should support detection and protection of data leaks even on image files through OCR technology with the Network DLP .	Cert of compliance from Vendor
20	The solution should be able to identify data leaked in the form unknown and kwon encrypted format like password protected word document and The solution should be able to identify malicious traffic pattern generated by Malware infected PC in order to prevent future data leakage by the malware	
21	The solution should be able to alert and notify sender, sender's manager and the policy owner whenever there is a policy violation, Different notification templates for different audience should be possible.	
22	The incident should include a clear indication of how the transmission or file violated policy (not just which policy was violated), including clear identification of which content triggered the match and should allow opening of original attachment directly from the UI	To be demonstrated by vendor & checked by BOO
23	The incident should display the complete identity of the sender(Full name, Business unit, manager name etc.) and destination of transmission for all endpoint channels. The solution should also allow assigning of incidents to a specific incident manager.	
24	The solution should provide automatic notification to incident managers when a new incident is assigned to them and the incident should not allowed for deletion even by the product administrator. The solution should allow a specific incident manager to manage incidents of specific policy violation, specific user groups etc.	
25	The solution should have role options for managing and remediating incidents. The system should allow a role only to view incidents but not manage or remediate them	To be demonstrated by vendor & checked by BOO
26	The system should control incident access based on role and policy violated. The system should also allow a role creation for not having rights to view the identify of the user and the forensics of the incident	
27	The system should create separate roles for technical administration of servers, user administration, policy creation and editing, incident remediation, and incident viewing for data at rest, in motion, or at the endpoint	
28	The system should have options to create a role to see summary reports, trend reports and high-level metrics without the ability to see individual incidents	
29	The solution should have a dashboard view designed for use by executives that can combine information from data in motion (network), data at rest (storage), and data at the endpoint (endpoint) in a single view. The solution should provide a single policy framework for not just Network and Endpoint DLP as well as Web and Email Security as well.	
30	The system should allow reports to be mailed directly from the UI and should allow automatic schedule of reports to identified recipients. The system should allow incident managers and administrators to use their Active directory credentials to login into the console	
31	The system should provide options to save specific reports as favorites for reuse and The reports should be exported to at least CSV, PDF, HTML formats. The system should have lots of pre-defined reports which administrators can leverage	
32	The system should allow automatic movement or relocation of file, delete files during discovery and The system should display the original file location and policy match details for files found to violate policy	
33	The system should leave the "last accessed" attribute of scanned files unchanged so as not to disrupt enterprise backup processes. The system should support incremental scanning during discovery to reduce volumes of data to be scanned	
34	The OEM should have own TAC center in India.	Cert of compliance from Vendor
35	The solution should Support PrtSc blocking on endpoint when configurable list of specific application are running, no matter it is in the foreground or background. The actual PrtSc capture will also be submitted to the DLP system as forensic evidence.	To be demonstrated by vendor & checked by

36	Incident manage the workflow of the selected incident, then select one of the following options Assign, Change Status, Change Severity, Ignore Incident, Tag Incident, Add Comments, Delete, Download Incident, Lock, unlock	BOO
37	A single event should trigger only one incident, even if it trigger multiple policy and violation. For example, an outbound email could trigger 5 policies, e.g. PCI-DSS, PII, etc, but only one single incident will be created. Solution should support CCN# display in violation trigger to be masked in order to stay compliance with PCI-DSS requirement.	
38	The solution should Support multiple conditions by combining different data classifier, including Policy Template, Patter, RegEx, Keyword, Dictionary, Natural Language Policy (NL) as well as Fingerprinting. For example : (A) ID# by policy template (B) CCN# by policy template (C) Name by fingerprinting (D) Address by fingerprinting And then create a policy with multiple matching conditions including (A and B) or (A and C) or (A and D)	To be demonstrated by vendor & checked by BOO
39	The solution should enforce fingerprinting policy on both network and endpoint channel, even when the endpoint is off network By using Python, complex logic, rating and algorithm can be developed as a custom data classifier where customer can use in compound with any existing data classifier to identify sensitive data which is unique to an organization	
40	The solution should have ability to detect cumulative malware information leaks through web channel.	
41	The solution should able to detect the data leaks over to competitors and the data sent and uploaded after the office hours predefined patterns.	
42	The solution should able to detect and Block the sensitive information uploads to Group of P2P software :- BitTornado Bittorrent eMule - eMule FrostWire	
43	Endpoint Should have the capability to contained files to temporary storage- to prevent sensitive information from being written from an endpoint to a removable device—such as a USB flash drive, CD/DVD, or external hard disk	
44	The solution should support the templates for detecting the Deep Web Urls- .i2P and .Onion , Encrypted attachments to competitors , Password Dissemination , User Traffic over time , Unknown Encrypted File Formats Detection.	
45	The solution should suport detection of PKCS #12 files (.p12, .pfx) that are commonly used to bundle a private key with its X.509 certificate.	
46	The solution should support the multiple Endpoint Profile Creation for the Better Security between the different departments. Encryption Keys are also should be isolated between the different departments.	
47	The endpoint installed should have the capacity to create the Bypass ID after validation by the administrator by generating the Passcode.	
48	Solution should support the Machine Learning and should be able to define the sensitivity of the classifiers.	
49	Solution should support the detecting and blocking the printing to the local or the Network Printer.	
50	Solution Should provide the User Awareness Confirm option when transferring the Sensitive content to Mass storage, User will define the justification and reason of doing the violation.	
51	The solution should have the capacity to monitors unencrypted data being copied to native Windows and Mac CD/DVD burner applications	
52	Endpoint should have the capacity to discover the Files that are modified between the specified Dates or Month Ago or Also for specific size to reduce the bandwidth and effective discovery.	
53	Solution should support detection and protection on data sharing on online medical applications from day 1:- · AllegianceMD · eClinicalWorks · ECLIPSYS · INGENIX · inteGreat · Sequel	

54	Solution should support fingerprint file systems, SharePoint servers, and Lotus Domino servers.	
55	Solution should have the option to define the applications that needs to be decoupled from the Endpoint and not scan.	
56	Solution Should support the HA for the Endpoint Servers - Primary , Secondary without any integration of 3rd party software.	
57	The solution must be present in the Gartner's leader quadrant for Data Loss Prevention for the past 7yrs.	

11. ANALYTICS AND MANAGEMENT END POINT

Ser No	Description of Requirements	Compliance
1	The solution should collect data through an endpoint agent that is capable of monitoring and collecting metadata for various types of behavior. At a minimum, behavior monitored should include: application usage, clipboard activity, email activity, file activity, keyboard activity, log on and log off events, printer activity, process activity, web browsing, and desktop video capture.	To be demonstrated by vendor & checked by BOO
2	The solution should be able to capture displayed text from any open application.	
3	The solution should be able to capture any text, images, or files copied to the clipboard.	
4	The solution should be able to capture email activity from both Outlook as well as common webmail vendors (Gmail, Hotmail, Yahoo, etc.) It should capture information about who the email was from, to whom it was sent, and any other recipients (cc or bcc). It should capture the subject line, the actual content of the message, and copies of any attached files.	
5	The solution should be able to capture information about file activity including reads, writes, copies. The solution should be able to capture the actual files involved in the activity.	
6	The solution should be capable of capturing all keyboard key strokes.	
7	The solution should be capable of recording all log on and log off events, including failed log on attempts.	
8	The solution should be capable of capturing information about any printer activity, including the document name, the printer name, and copies of the actual document(s) sent to print.	
9	The solution should be capable of capturing information about any processes started or stopped.	
10	The solution should be capable of capturing the rendered HTML from any websites visited.	
11	The solution should capture DVR-like desktop video. The solution should also support the ability to customize the way desktop video collected is stored, including presenting the option of storing it in gray scale and adjusting the frame rate. Frame rate should be available at a rate of at least four frames per second.	
12	When the user is not connected to the internet, all collected data should be stored in a local disk cache on the endpoint and sent to the server as soon as it is again connected. This data should be capable of being sent to the server regardless of whether the endpoint is on or off the network.	
13	The endpoint should throttle the rate at which data is sent to the server to avoid a large impact on network performance.	
14	The endpoint agent should be able to detect and prevent tampering with the endpoint agent. It should be capable of generating an event if a user attempts to do so.	
Endpoint Management		
15	The solution should provide a way to manage the endpoints installed. It should be capable of sending commands to those endpoints.	To be demonstrated by vendor & checked by BOO
16	The solution should provide a way to deploy endpoints with a select subset of functionality in order to maintain privacy requirements for specific individuals, groups, departments, or countries.	
17	The solution should provide a way to assign individual endpoints and/or individuals to groups to facilitate easier management.	
18	The solution should provide a way to monitor the health and connectivity of the endpoints.	

Policy Engine		
19	The solution should provide a user interface for creating policies that can be selectively deployed to groups of endpoints or users. These policies should govern which data is collected and under what circumstances it is collected.	To be demonstrated by vendor & checked by BOO
20	Policies should allow for filtering and pre-filtering of data to determine the appropriate action. This includes searching any collected data for specific keywords or patterns matching regular expressions.	
21	Policies should be able to govern what data is cached and stored locally on the endpoint unless specifically requested, and what data is automatically sent up to the server as soon as it is collected.	
22	Policies should be able to define scenarios where data will not be collected despite the rules of other policies.	To be demonstrated by vendor & checked by BOO
23	The solution should have several sets of policies that meet common use cases readily available.	
24	The solution should allow for policies to trigger an email notification.	
25	The solution should allow for information to be automatically sent to a SIEM when certain policies are violated.	
Investigation		
26	The solution should allow for searching and filtering of all collected data. If files or video have been collected, those items should also be made available for review.	To be demonstrated by vendor & checked by BOO
27	The solution should allow for various pieces of collected information to be grouped together into a case.	
28	The solution should provide a status on the various events and record when the event is either cleared or escalated for further review.	
29	The solution should perform analytics to automatically assign users a risk score. The risk score should identify anomalous user behavior and surface a short list of the most risky users for review.	
30	The solution should allow for individual policies to receive a weighting that controls how much they contribute to the risk score.	
31	The solution should clearly explain how different components of the scoring model contributed to a user's risk score.	

12. DATA LEAKAGE PROTECTION GATEWAY

Ser No	Required Technical Descriptions	Compliance
	Data Security	
	Network Data & Cloud Monitoring and Prevention	
1	The solution should detect and prevent content getting posted or uploaded to specific websites, blogs, and forums accessed over HTTP, HTTPS. The solution should be able to enforce policies by URL's, domains or URL categories either natively or by integrated Web Security solution. The solution should be able to monitor FTP traffic including fully correlating transferred control information and should be able to monitor IM traffic even if its tunneled over HTTP protocol.	To be demonstrated by vendor & checked by BOO
2	The DLP Solution must have capability to integrate with 3rd party Proxy solution for content inspection using ICAP channel or must have DLP engine on OEM provided Proxy itself	
3	The solution should be able to block outbound emails sent via SMTP if its violates the policy	
4	The proposed solution work as a MTA to receive mails from mail server and inspect content before delivering mails to next hop and should quarantine emails that are in violation of company policy.	
5	The solution should be able to prevent content getting posted or uploaded to destinations (Web, Email domains etc..) and should monitor and control sensitive emails downloaded to mobile devices through ActiveSync	
6	The solution should support Email DLP deployment in Microsoft Azure for Office 365. All licenses required for the same should be included and management should be from the same centralized management platform	
7	The solution should be able to identify data leaked in the form unknown and kwon encrypted format like password protected word document. The solution should be able to identify malicious traffic pattern generated by Malware infected PC in order to prevent future data leakage by the malware. The solution should support quarantine as an action for email policy violations and should allow the sender's manager to review the mail and provide permissions for him	

	to release the mail without logging into the UI	To be demonstrated by vendor & checked by BOO
8	The DLP Solution must natively integrate with Cloud solutions like One Drive as well as Box to monitor uploads as well as sharing of data from different assets connected outside the organization. This must be outside endpoint DLP solution.	
	Data Identification & Policy Management	
9	The solution should have a comprehensive list of pre-defined policies and templates with over 1700+ patterns to identify and classify information pertaining to different industry like Energy, Petroleum industry vertical etc and India IT Act.	To be demonstrated by vendor & checked by BOO
10	The solution should provide capabilities to identify data based on keywords or dictionaries and the solution should be able to enforce policies based on file types, size of files and also the name of the file	
11	The solution should be able to detect and block encrypted and password protected files without reading the encrypted content.	
12	The solution should be able to do full binary fingerprint of files and also should be able to detect even if partial information gets leaks from fingerprinted files or folders	
13	The solution should be able to recursively inspect the content of compressed archives	
14	The solution should be able to fingerprint only specific fields or columns within a database and should be able to identify information from databases by correlating information residing in different columns in a database	
15	The Solution should have advanced Machine Learning – Ability to automatically learn sensitive information from copies of information that needs to be protected and also automatically learn false positives.	
16	The solution should enforce policies to detect low and slow data leaks	
17	The solution should be able to enforce policies to detect data leaks even through image files through OCR technology.	
18	The solution should be able to identify data leaked in the form unknown and known encrypted format like password protected word document	
19	The solution should be able to identify and block malicious activity like data thefts through files encrypted using non-standard algorithms.	
20	The Proposed DLP Solution must be GDPR Compliant	Cert of compliance from Vendor
21	The proposed DLP Solution must be able to detect Data Classification Labels applied by Data Classification partners by reading metadata as well as custom header analysis.	To be demonstrated by vendor & checked by BOO
22	The solution should support the templates for detecting the Deep Web Urls- .i2P and .Onion , Encrypted attachments to competitors , Password Dissemination , User Traffic over time , Unknown Encrypted File Formats Detection. The solution should support detection of PKCS #12 files (.p12, .pfx) that are commonly used to bundle a private key with its X.509 certificate.	
	Automated Response & Incident Management	
23	The solution should be able to alert and notify sender, sender's manager and the policy owner whenever there is a policy violation, Different notification templates for different audience should be possible.	
24	The solution should support quarantine as an action for email policy violations and should allow the sender's manager to review the mail and provide permissions for him to release the mail without logging into the UI	
25	The incident should include a clear indication of how the transmission or file violated policy (not just which policy was violated), including clear identification of which content triggered the match and should allow opening of original attachment directly from the UI	
26	The incident should display the complete identity of the sender(Full name, Business unit, manager name etc.) and destination of transmission for all network and endpoint channels. The solution should also allow assigning of incidents to a specific incident manager	
27	The solution should provide automatic notification to incident managers when a new incident is assigned to them and the incident should not allowed for deletion even by the product administrator	

28	The solution should allow a specific incident manager to manage incidents of specific policy violation, specific user groups etc.	
29	The solution should have options for managing and remediating incidents through email by providing incident management options within the in the notification email itself.	
	Role Based Access and Privacy Control	
30	The system should control incident access based on role and policy violated. The system should also allow a role creation for not having rights to view the identify of the user and the forensics of the incident	
31	The system should create separate roles for technical administration of servers, user administration, policy creation and editing, incident remediation, and incident viewing for data at rest, in motion, or at the endpoint	To be demonstrated by vendor & checked by BOO
32	The system should allow a role only to view incidents but not manage or remediate them	
33	The system should have options to create a role to see summary reports, trend reports and high-level metrics without the ability to see individual incidents	
34	The system should allow incident managers and administrators to use their Active directory credentials to login into the console	
	Reporting and Analytics	
35	The solution should have a dashboard view designed for use by executives that can combine information from data in motion (network), data at rest (storage), and data at the endpoint (endpoint) in a single view	
36	The system should allow reports to be mailed directly from the UI and should allow automatic schedule of reports to identified recipients	
37	The reports should be exported to at least CSV, PDF, HTML formats	
38	The system should provide options to save specific reports as favorites for reuse	
39	The system should have lots of pre-defined reports which administrators can leverage	
40	The proposed solution should provide Incident Workflow capabilities where user/Business Manager can remediate the DLP policy violations actions from handsets/emails without logging into the Management Console	
41	The DLP Solution must provide visibility into Broken Business process. For ex:- if unsecured sensitive content is sent daily from several users to a business partner, the users are probably not aware that they are doing something wrong.	
42	The Proposed DLP engine must performs a post-processing incident grouping step to avoid displaying related incidents in different cases. All incidents from the same user that have the same classification are combined into a group and DLP case card.	
43	The DLP dashboard must display the number of cases in the designated period that fall above the risk score threshold that you've selected. Risk score thresholds must be customizable and instantly produce an report to prioritize the cases from high-to-low risk levels by leveraging analytics or machine learning technologies.	
	Storage (Data at rest)	
44	The system should allow automatic movement or relocation of file, delete files during discovery	
45	The system should display the original file location and policy match details for files found to violate policy	
46	The system should leave the "last accessed" attribute of scanned files unchanged so as not to disrupt enterprise backup processes	
47	The system should support incremental scanning during discovery to reduce volumes of data to be scanned.	
	Management Monitoring	
48	The solution should have centralized management and unified policy enforcement platform.	
49	The solution should provide detailed reporting and if database is required for reporting then please provide hardware/software requirements for the same	
	Supports Third part recognitions	
50	The solution must be present in the Gartner's leader quadrant for Data Loss Prevention for the past 7yrs.	Cert of compliance from Vendor
51	The OEM should have own technical support center in India.	

13. ANALYTICS AND MANAGEMENT SERVER

Ser No	Description of Requirements	Compliance
1	Must prioritize/score user risk activity and display highest risk users on enterprise watch dashboard	To be demonstrated by vendor & checked by BOO
2	Must support drill down capability to all supporting forensic events contributing to the overall behavioral risk.	
3	Drill down must support e-mail and chat communication reconstruction	
4	Drill down must show individual event feature scores that contributed to overall model risk score.	
5	Must be able to reconstruct e-mail for NLP Forensics investigation of risk indicators	
6	Must be able to see all associated network activity associated with a key risk indicator	
7	Must be able to navigate the spread of sensitive information throughout the enterprise.	
8	Must be able to capture all related Forensics supporting data for case investigation purposes	
9	Must provide evidence, analysis, and information to support incident response and remediation	
Multi-Channel and Multi-Network Analytic Scenarios		
10	Must be able to correlate system activity across discrete networks (e.g. same user on classified and unclassified networks).	To be demonstrated by vendor & checked by BOO
11	Must support a layered risk score comprised of behavior anomaly analytics monitoring separate data channels (e.g. file copy, file print, file upload, file download)	
12	Must be able to correlate interactions across people, data, devices, and applications	
Custom Analytic Model Development and Management Interface		
13	Must be able to develop complex user behavior analytic models through a simple to use graphical user interface.	To be demonstrated by vendor & checked by BOO
14	Must be able to support model modification and administration through a simple to use graphical user interface.	
15	Must be able to modify risk score weighting on specific model features through a simple to use graphical user interface.	
Out Of The Box Insider Threat Analytics Model Library		
16	Collection of analytic models tuned to detect sensitive data exfiltration	To be demonstrated by vendor & checked by BOO
17	Collection of analytic models tuned to detect a malicious user	
18	Collection of analytic models tuned to detect negative behavior and models tuned to detect -Workplace Violence -Radicalized Actor -Sexual Harassment -Suicide Risk	
19	Collection of analytic models tuned to detect illicit behavior - Specific models tuned to detect illegal activity - Specific models tuned to detect violation of DoD IT security policy	
20	Collection of analytic models tuned to detect compromised user account	
High Performance - Pre built and Easily Customizable - Data Ingest Connectors		
21	data ingest connectors are configurable through a graphical user interface for rapid configuration to customer specific data sources	To be demonstrated by vendor & checked by BOO
22	Should offer a highly scalable deployment architecture critical for high volume streaming data ingest	
23	Should allow for highly scalable data enrichment for any network event during real time data ingestion (for example: as IP address is captured during a network event, the UEBA solution can utilize agency specific threat intelligence feeds to enrich a file upload or download event).	

24	Should have pre built connectors for the following categories at the least - SIEM (Splunk, Arcsight, IBM, RSA) - Communications (Exchange, Skype, Symphony, bloom berg) - User Access and System Administration (Windows, Linux) - DLP (Forcepoint, Symantec, McAfee, Digital Guardian) - UAM (Forcepoint, digital Guardian, Dtex) -Entity Information (AD, CMDB, Workday, Sales force etc) - Proxy (Forcepoint, Bluecoat, Cisco, F5) -Physical Data movement (Print logs, Removale media logs)	To be physically checked by BOO
Unstructured AND Structured Data Analytics		
25	Must support search and NLP analytics on content of communication data	To be demonstrated by vendor & checked by BOO
26	Must support search and NLP analytics on content of attachments associated with e-mail	
27	Must support search NLP analytics on web browser queries	
28	Must support search and NLP analytics on file content associated with print jobs	
29	NLP analytics Must be able to detect - Flight risk indicators - Negative sentiment indicators - Workplace violence indicators - Radicalized actor indicators - Sexual harassment indicators - Harm to self indicators	
Human Risk Data Analytics		
30	HR indicators for poor performance or workplace reprimand	To be demonstrated by vendor & checked by BOO
31	IT policy violation	
32	Standard CI Adjudicative data sources (legal, financial, foreign travel, etc.)	
Investigation Collaboration & Management		
33	Tracking and sharing investigator comments on high-risk entities and events of interest	To be demonstrated by vendor & checked by BOO
34	Grouping and organizing high-risk events together to form a case	
35	Escalating high-risk activities for other application users to review and/or investigate	
36	Exporting event information from the application for use in external case management systems	
Endpoint UEBA		
37	The solution should collect data through an endpoint agent that is capable of monitoring and collecting metadata for various types of behavior. At a minimum, behavior monitored should include: application usage, clipboard activity, email activity, file activity, keyboard activity, log on and log off events, printer activity, process activity, web browsing, and desktop video capture.	To be demonstrated by vendor & checked by BOO
38	The solution should be able to capture displayed text from any open application.	
39	The solution should be able to capture any text, images, or files copied to the clipboard.	
40	The solution should be able to capture email activity from both Outlook as well as common webmail vendors (Gmail, Hotmail, Yahoo, etc.) It should capture information about who the email was from, to whom it was sent, and any other recipients (cc or bcc). It should capture the subject line, the actual content of the message, and copies of any attached files.	
41	The solution should be able to capture information about file activity including reads, writes, copies. The solution should be able to capture the actual files involved in the activity.	
42	The solution should be capable of capturing all keyboard key strokes.	
43	The solution should be capable of recording all log on and log off events, including failed log on attempts.	
44	The solution should be capable of capturing information about any printer activity, including the document name, the printer name, and copies of the actual document(s) sent to print.	
45	The solution should be capable of capturing information about any processes started or stopped.	

46	The solution should be capable of capturing the rendered HTML from any websites visited.	To be demonstrated by vendor & checked by BOO
47	The solution should capture DVR-like desktop video. The solution should also support the ability to customize the way desktop video collected is stored, including presenting the option of storing it in gray scale and adjusting the frame rate. Frame rate should be available at a rate of at least four frames per second.	
48	When the user is not connected to the internet, all collected data should be stored in a local disk cache on the endpoint and sent to the server as soon as it is again connected. This data should be capable of being sent to the server regardless of whether the endpoint is on or off the network.	
49	The endpoint should throttle the rate at which data is sent to the server to avoid a large impact on network performance.	
50	The endpoint agent should be able to detect and prevent tampering with the endpoint agent. It should be capable of generating an event if a user attempts to do so.	

14. WEB SECURITY GATEWAY

Ser No	Description of Requirements	Compliance
1	The solution should provide proxy, caching, on box malware inspection, content filtering, SSL inspection, protocol filtering and inline AV in block mode on the same Appliance.	To be demonstrated by vendor & checked by BOO
2	The Solution should be designed for user base in active-active mode managed through centralized management console on server platform.	
3	The Solution should provide HA and Load balancing functionality in Secure web gateway solution with or without any dependency on pac, external load-balancer or dns round-robin methods	
4	The solution should have complete license for Antivirus ,SSL, web security and content inspection and control should be built in solution for user base from the first day in same appliance. The Solution should intercepts user requests for web destinations (HTTP,HTTPs,and FTP) for web security and in-line AV scanning.	
5	The proposed solution should be able to inspect malicious information leaks even over SSL by decrypting SSL natively .The proposed SSL solution should be part of Gartner's Leaders/Challengers quadrant.	
6	The solution should be capable of dynamically blocking a legitimate website which has become infected and unblock the site in real time when the threat has been removed for below mentioned security categories and vulnerabilities.	
7	so Solution vendor should ensure to provide below mentioned security categories from day1 with automatic database updates for security categories- Advanced malware command and control, Advanced malware payloads, Bot networks, Compromised websites, key loggers, Phishing and other frauds, Spywares	
8	The solution should inspect the sensitive content through pre-defined templates, textual content inside image, cumulative content control and inspection through web channel.	
9	The solution should have ability to protect the sensitive data exhilaration based on geo-location.	
10	The solution should be able to scan files, folders, databases and prevent the content from being sent over outbound web channel. The solution should have ability to provide geo-location awareness for security incidents	
11	The solution should have at least 20+ million websites in its URL filtering database and' should have pre-defined URL categories and application protocols along with YouTube, Facebook and linked-in controls. Solution vendor should ensure that 100 predefined categories & 100+ pre-defined protocols should be available on product from day-1. Also in-addition solution should have ability to configure custom categories for organization.	Cert of compliance from Vendor
12	The solution should have partnerships or third party inputs for web threat ratings from Virus total or Facebook	

13	The solution must detect and block outbound Botnet and Trojan malware communications. The solution must log and provide detailed information on the originating system sufficient to enable identification of infected units for mitigation	To be demonstrated by vendor & checked by BOO
14	The solution should support same policy enforcement in real time policy sync for users even when they access Internet outside the corporate network, this should be enforced through an agent deployment on roaming endpoints ((MAC/Windows) . And this solution should be on premises and not with the help of SAAS i.e. mobile user traffic should redirect to on-premise solution for policy checks. As per the security guidelines no SaaS or policy server public publishing should be allowed for the same.	
15	The agent on the roaming user machines should be tamperproof, for example, the agent cannot be uninstalled by the user even with admin rights to the system or the user cannot stop the services	To be demonstrated by vendor & checked by BOO
16	The solution should have ability to block anonymizer sites or proxy avoidance tools. Below mentioned tools should be blocked from first day and should be provided in default protocol database Ghostsurf, Google web accelerator, Hopster, Jap, Realtunnel, Socksonline, Tongtongtong, Toonel, Tor, Yourfreedom.	
17	Solution should provide separate Management server which can push policies for centralized management and reporting in case of multiple site solution deployment. Management console should provide automatic policy sync to all the remote boxes when the change is made to central console. Centralized management and centralized reporting console can be appliance based or software server hardware based but no VM should be used for the same.	
18	MAC OS X 10.10 and MS Windows 10 support for mobile laptop users web filtering client.	
19	The solution should have cloud application usage and associated risk visibility.	
20	The solution should apply security policy to more than 100 protocols in multiple categories more than 15. This includes the ability to allow, block, log, and assign quota time for IM, P2P, and streaming media and solution should provide at least below mentioned security categories as below RIGHT FROM FIRST DAY:1)Advanced Malware Command and Control category 2)Advanced Malware payload detection category 3)Malicious embedded links and iframe detection category 4)Mobile malware category 5)Key logger and Spyware category 6)P2P software database from day 1 to control/block the below P2P protocols	
21	The solution should filter out embedded objectionable or unproductive content, this includes examination of the source server, URL, page content, and active content. The solution should have functionality to control web 2.0 and real time content categorization.	
22	The solution should have granular control over popular social web applications like Facebook, LinkedIn, Twitter, YouTube, and others. The solution should have social control Video UPLOADS to Facebook and YouTube applications.	
23	The solution must provide below mentioned categories or similar to functionally for Facebook control from day 1 Facebook Posting: Facebook function that enables a user to share a post, status or link, Facebook Commenting, Facebook Friends, Facebook Photo Upload, Facebook Mail, Facebook Events, Facebook Apps, Facebook Chat, Facebook Questions, Facebook Video Upload, Facebook Groups etc	
24	The solution should have built-in or custom policies for identifying and segregate You Tube traffic for Education only and Other irrelevant non-compliance video, It should simplify design and implementation of policy to ensure user compliance.	
25	The solution should provide geo-location awareness for security incidents. The solution should provide inbuilt capability malicious content of password and unknown encryption files.	
26	The solution should be able to manage the complete solution through centralized management and reporting console which should be software or appliance based.	

27	The solution should support to have capability to differentiate between YouTube educational and entertainment videos through default categories and should have separate default categories for the same.	To be demonstrated by vendor & checked by BOO
28	The solution should have authentication options for administration, the specific permissions available depend on the type of administrator and Administrator activity is logged and available for auditing or troubleshooting.	
29	The solution should have authentication options for users/groups, It should supports authentication of users via Integrated Windows Authentication (Kerberos), NTLM (NTLM v1 and v2 in Session Security), and LDAP.	
30	The solution should have support of multiple domains, the administrators can specify the sequence (Domain controllers checked first, second, next, etc.) used to authenticate users who login from different locations.	
31	The solution should supports credential caching (for transparent and explicit proxy) to reduce load on domain controllers.	To be demonstrated by vendor & checked by BOO
32	The solution should have Multi-Domain authentication to allow the admin to create rules that authenticate against multiple domain controllers in a sequence	
33	The solution should have centralized management for multiple web egress points The solution should support for two factor Authentication for Management Server.	
34	The solution should support real time graphical and chart based dashboard for the summary of web filtering activities. The solution should pre-built report templates which the administrator can use for generating reports.	
35	The solution should have capabilities to automatically deliver reports based on schedule to selected recipients. The solution should support custom report creation in Excel and PDF.	
36	The solution should be able to consolidate reports from multiple boxes for centralized logging and reporting. The solution should provide detailed information on security incidents to comprehensively investigate individual threat events	
37	The solution should be integrated to third-party SIEM applications like syslog/CEF (ArcSight), syslog key-value pairs (Splunk and others), syslog LEEF (QRadar), and Custom.	
38	The solution should provide a Web UI to manage Internet usage policies, it should also support delegated administration and reporting capabilities so different roles can be created to manage policies and view reports.	
39	The solution should provide native system health monitoring, alerting and troubleshooting capabilities. The solution should provide reports based on hits, and bandwidth.	
40	The solution should support configuring scheduled automatic backup of system configuration. The solution should support automatic download of available patches or fixes	
41	The Solution should have inbuilt reporting feature like real time monitoring, reporting templates and investigation drill down report. The solution should have reporting on the user agent strings of applications to provide details on application usage and version details including browser version reports.	
42	The solution should be able to block back channel communication of sensitive data through default 1500 templates.	
43	The solution should have visibility and control for cloud applications and shadow IT application usage	
44	The OEM Should in the Gartner leaders/challenger Quadrant for Secure web gateway solution. The OEM should have own T AC centre in India.	Cert of compliance from Vendor

15. INSIDENT RESPONSE MANAGEMENT AND ALERT SERVER

Ser No.	Description of Requirements	Compliance
	General Requirement of IT Service Management Solution:	
1	Should able to support and handle large volume of incident	Cert of compliance from Vendor
2	Should able to support and handle large volume of service requests	
3	Should able to support and handle large volume of changes	
4	Proposed Service desk/ HDMS must be ITIL certified	
5	Native integration of processes i.e. Incident Management with Change Management and vice-versa	To be demonstrated by vendor & checked by BOO
6	Native integration of processes with Knowledge base i.e. automatically creation of knowledge base post closure of tickets	
7	The solution should have a Single Architecture and leverage a single application instance across ITIL processes, including unique data and workflows segregated by business unit.	
8	Able to create and modify forms as per customer requirement	
9	Able to define different SLAs for different services / domains	
10	Solution should support multi-tenancy with complete data isolation as well as with ability for analysts based on access rights to view data for one, two or more organizational units	
11	Able to define different workflows for different processes	
12	Able to send automatic escalation mails as defined in workflow	
13	Should be able to integrate CMDB from different federated data sources and build a single CMDB	To be demonstrated by vendor & checked by BOO
14	Should provide email based interactions allowing ticket creation, update and approval of request.	
15	Should able to integrate with Active Directory and populate user information automatically	
16	The system should have graphical interface to define, visualize and update ITIL processes	
17	The solution should provide to browse through CMDB which should offer powerful search capabilities and auto-completion for configuration items and services, enabling to quickly find Cis as well as their relationships to other Cis.	
	Incident and Problem Management	
18	Service Desk solution should allow detailed multiple levels/tiers of categorization on the type of incident being logged for IT services that shall span across multiple domains.	To be demonstrated by vendor & checked by BOO
19	Service Desk solution should provide classification to differentiate the criticality of the security incident via the priority levels, severity levels and impact levels.	
20	The solution should provide embedded and actionable best practices workflows i.e., best-practices process & views based upon implementations	
21	It should allow SLA to be associated with a ticket based on priority, severity, incident type, requestor, asset, location.	
22	Solution should support fast service restoration leveraging previous incident data.	
23	It should have the ability to search multiple built-in knowledge bases like the incident, problem, and known-error database simultaneously without requiring the agent to search each knowledge base individually.	
24	Should support automatic assignment of ticket to the right skilled resource based on business priority Ex – Database crash issue need not be assigned to an L3 DBA unless the business service is completely down	
25	It should have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.	
26	Should support text search capabilities	
27	Should centralize all known error and problem workarounds into a single, searchable knowledge base	
28	It should provide an interactive process flow bar that guides novice users through the ITIL process for incident management to ensure faster issue resolution.	
29	The incident Management solution should be completely integrated to the CMDB to ensure that Cis can be associated with the ticket to provide better visibility	

30	The incident management solution should have the ability to initiate the change request	
31	The solution should have the ability to associate an incident with an existing change request, a problem or known error for tracking purposes	
32	The service desk should have shift management capabilities for support staff wherein tickets are allocated based on shift availability.	
33	It should allow the CI to be associated with tickets.	

16. NETWORK ACCESS CONTROL

Ser No	Description of Requirements	Compliance
	COMPREHENSIVE LAN SECURTIY	
	The proposed solution should match following criteria:-	
1	Total 6 number fixed 10/100/1000 interface as part of supply from day 1.	To be physically checked by BOO
2	Total 1 No. of Flexi Port. Flexi Port should Support 8 port GE copper/8 port GE SFP/ 2 port 10 GE SFP+ Modules (Optional if required).	
3	Hard drive (local quarantine/logs) : 120 GB	
4	Firewall Throughput should be 18 Gbps or more	To be demonstrated by vendor & checked by BOO
5	VPN Throughput should be 1.5 Gbps	
6	IPS Throughput should be 4.2 Gbps or more	
8	Concurrent Connections should be 4,000,000	
9	New Connections /Sec should be 60,000	
10	Maximum Licensed Users should be unrestricted	
11	The Firewall/UTM should be leader in Gartner Magic Qudrant for Unified Threat Management since last three years.	Cert of compliance from Vendor
12	**General Management**	
13	Customizable Dashboard and SNMP Support	To be demonstrated by vendor & checked by BOO
14	Role Based Administration	
15	Software/Hardware Based UTM Manager to manage multiple UTM devices.	
16	Manually Or fully automated backup & restore options	
17	Self service user portal for one click vpn setup	
18	Reusable System Object Definitions for networks, services, hosts, users & groups.	
19	**Firewall**	
20	The proposed solution should be standalone appliance with hardened OS.	To be demonstrated by vendor & checked by BOO
21	The proposed solution should be ICSA certified firewall.	
22	Should Support NAT static, masquerade (dynamic).	
23	Should Support Full configuration of DNS, DHCP and NTP	
24	Should Support Routing: static, multicast (PIM-SM) and dynamic (BGP, OSPF)	
25	Should Support WAN link balancing: Internet connections, auto-link health check, automatic failover, automatic and weighted balancing and granular multipath rules	
26	Should Support QoS with full control over bandwidth pools and download throttling using Stochastic Fairness Queuing and Random Early Detection on inbound traffic.	
27	Should Have IPv6 support	
28	Should Support VoIP handling for SIP and H.323 connections	
29	Should Have Reverse Proxy & URL Hardening Engine	
30	Should Have Deep-linking control, Directory traversal prevention, SQL injection protection ,Cross-site scripting protection.	
31	HTTPS (SSL) encryption offloading	
32	**IPS**	
33	Intrusion protection: Deep packet inspection engine, 12,000+ patterns	

34	Should Have Selective IPS patterns for maximum performance and protection	To be demonstrated by vendor & checked by BOO
35	Should Support IPS pattern aging algorithm for optimal performance	
36	Should Have Flood protection: DoS, DDoS and portscan blocking	
37	Should Support Country blocking by region or individual country (over 360 countries) with separate inbound/outbound settings and exceptions	
38	**Advanced Threat Protection**	
39	Should Detect and block network traffic attempting to contact command and control servers using DNS, AFC, HTTP Proxy and firewall	To be demonstrated by vendor & checked by BOO
40	Should Identify infected hosts on the network and contain their network activity	
41	Should Have Selective sandboxing of suspicious code to determine malicious intent	
42	**Web Protection**	
43	URL Filter database with 30 million+ sites in 95 categories and 64+ languages	Cert of compliance from Vendor
44	Application Control: Accurate signatures and Layer 7 patterns for thousands of applications	
45	Dynamic application control based on productivity or risk threshold	To be demonstrated by vendor & checked by BOO
46	View traffic in real-time, choose to block or shape	
47	Malware scanning: HTTP/S, FTP and web-based email via dual independent antivirus engines block all forms of viruses, web malware, trojans and spyware	To be demonstrated by vendor & checked by BOO
48	Fully transparent HTTPS filtering of URLs	
49	Advanced web malware protection with JavaScript emulation	
50	Live Protection real-time in-the-cloud lookups for the latest threat intelligence	
51	Potentially unwanted application (PUA) download blocking	
52	Malicious URL reputation filtering backed by Global Labs	
53	Reputation threshold: set the reputation threshold a website requires to be accessible from internal network	
54	Active content filter: File extension, MIME type, JavaScript, ActiveX, Java and Flash	
55	YouTube for Schools enforcement	
56	Should Have Safe Search enforcement	
57	Should Support Authentication: Active Directory, eDirectory, LDAP, RADIUS, TACACS+ and local database	
58	Custom categorization to override categories or create custom categories	
59	Policy testing tool for URLs, times, users and other parameters	
60	Customizable block pages	
61	**Email Protection/ Anti Spam**	
62	Reputation service with spam outbreak monitoring based on patented Recurrent- Pattern-Detection technology	To be demonstrated by vendor & checked by BOO
63	Advanced spam detection techniques: RBL, heuristics, SPF checking, BATV, URL scanning, grey listing, RDNS/HELO checks, expression filter and recipient verification	
64	Block spam and malware during the SMTP transaction	
65	Detects phishing URLs within e-mails	
66	Global & per-user domain and address black/white lists	
67	Recipient Verification against Active Directory account	
68	E-mail scanning with SMTP and POP3 support	
69	Dual antivirus engines	
70	Archived and compressed attachment scanning with deep-level support	

71	Scan embedded mail formats: Block malicious and unwanted files with MIME type checking	To be demonstrated by vendor & checked by BOO
72	Quarantine unscannable or over-sized messages	
73	Filter mail for unlimited domains and mailboxes	
74	Automatic signature and pattern updates	
75	Patent-pending SPX encryption for one-way message encryption	Cert of compliance from Govt Auth Lab/OEM
76	Completely transparent, no additional software or client required for Email Encryption.	To be demonstrated by vendor & checked by BOO
77	PGP key server support	
78	Allows content/virus scanning even for encrypted e-mails	
79	DLP engine with automatic scanning of emails and attachments for sensitive data	
80	User-quarantine reports mailed out daily at customizable times	
81	Customizable User Portal for end-user mail management, in 15 languages	
82	PDF and CSV exporting of reports	
83	Customizable email footers and disclaimers	
84	**VPN**	
85	PPTP, L2TP, SSL, IPsec, HTML5-based and Cisco client-based remote user VPNs, as well as IPsec, SSL, Amazon VPC-based site-to-site tunnels	To be demonstrated by vendor & checked by BOO
86	Authentication: Pre-Shared Key (PSK), PKI (X.509), Smartcards, Token and XAUTH	Cert of compliance from Vendor
87	Encryption: AES (128/192/256), DES, 3DES (112/168), Blowfish, RSA (up to 2048 Bit), DH groups 1/2/5/14, MD5 and SHA-256/384/512	Cert of compliance from Govt Auth Lab/OEM
88	Intelligent split-tunneling for optimum traffic routing	To be demonstrated by vendor & checked by BOO
89	NAT-traversal support	
90	Client-monitor for graphical overview of connection status	
91	Multilingual: German, English and French	
92	IPsec Tunnel Binding	
93	Sould Support Proven SSL-(TLS)-based security	
94	Ssl VPN Should have support for iOS and Android	
95	Should Have True clientless HTML5 VPN portal for accessing applications securely from a browser on any device	
96	**Logging & Reporting**	
97	Logging: Remote syslog, nightly rotation, email/ftp/ SMB/SSH archiving and log management service	To be demonstrated by vendor & checked by BOO
98	On-box reporting: Packet filter, intrusion protection, bandwidth and day/week/month/year scales	
99	Hundreds of on-box reports	
100	Per-user tracking and auditing	
101	Web log searching parameters per user, URL or action	
102	Full transaction log of all activity in human-readable format	
103	PDF and CSV exporting of reports	
104	Executive report scheduling and archiving	
105	**High Availability**	
106	The system shall support Zero-config active/active, active/passive high-availability.	

17. SECURITY SERVER

Ser No	Description Of Requirements	Compliance
1	**Separation of Duty and Privileged User Access Control**	
(a)	The solution must be able to protect data-at-rest against root/system privileged user account access. It should also protect file level encryption.	To be demonstrated by vendor & checked by BOO
(b)	Proposed data protection solution must support fine-grained policy to enable administrator to perform activity like file archive and backup, without access to the data content itself.	
(c)	The proposed solution must support a separation of duties(SoD) to meet rigorous compliance rules including PCI DSS, HIPAA/HITECH and government data breach policy. The vendor must provide compliance whitepaper to prove such support capability	
(d)	Proposed solution must support multi-tenancy using separate domain with configurable policies, data encryption key management and audit log. Must have a semaless SIEM Integration. Must Protect the unstructured data (file-shares, files and folders) including big data.	
2	**Support Transparent Data Encryption**	
(a)	The proposed data protection and encryption solution must support transparent data protection on all major operating system include: • Microsoft: Windows Server, 2008, 2012 • Linux: Red Hat Enterprise Linux (RHEL), SuSE Linux Enterprise Server, Oracle RedHat Compatible Kernel and Ubuntu • UNIX: IBM AIX, HP-UX, and Solaris Database	Cert of compliance from Vendor
(b)	there should not be any changes in the storage space after the encryption.	
(c)	Proposed data protection solution must be able to secure both structure database information and unstructured files such as PDF, spreadsheet, scripts, images, audio/video recordings and extract-transformation-load batch files..	Cert of compliance from Vendor
(d)	Proposed data security solution should have minimum performance impact to database transactions with not more than 10% performance overhead on transactions. Vendor must provide benchmark report to prove the performance claim	
(e)	The data transformation should not involve any downtime and live transformation is expected to achieve high Performance Encryption with 100% System Uptime. - Solution must be able to enforces access controls based on – “resources”, “processes”, and “time based access” so that only the defined resources can be accessed with the defined processes and defined users/groups at any given time - Ability to learn the effect of policies (learn mode) before actual encryption is applied is must. -Not only appliance but agent also needs to be FIPS certified	
3	**Application Encryption and Tokenization**	
(a)	The data protection solution must support format preserving tokenization	Cert of compliance from Vendor
(b)	the proposed tokenization and masking solution must provide REST API	
(c)	The data masking solution must support dynamic masking through policy based masks	
(d)	The proposed solution should support Teradata V14 and V14.1 database encryption with UDF	
(e)	The propsed platform should support vaultless tokenization	
(f)	The propsed platform should support vault based tokenization	
(g)	The propsed platform should support gateway to encrypt data stored on S3 and Box	
4	**Key Management and KMIP**	
(a)	the proposed encryption and key management solution must be able to support KMIP client	Cert of compliance from Vendor
(b)	The proposed solution should be certified to support Nutanix KMIP	
(c)	the proposed solution must provide centralized key management for Oracle and MSSQL TDE master key.	
(d)	The security administrator console should support 2-factor authentication with RSA.	

(e)	The data protection solution must provide centralized audit for security adminstration access, key creation, policy changes, data access log and so on.	Cert of compliance from Vendor
(f)	The proposed solution must provide application encryption support with Java, C/C++, and .Net API.	
(g)	The proposed solution support LDAP and Microsoft Active Directory authentication	
(h)	Support industry proven cryptograph security standard:3DES, AES128, AES256, ARIA128, and ARIA256 and asymmetric key RSA-4096/2048, SHA-256 algorithm	Cert of compliance from Govt Auth Lab/OEM
(j)	The Key management repository must provide virtualization option, with OVF image for deployment option - Hardened Operating System, root account must be disabled, all unnecessary software packages must be removed. A firewall in place that only opens a limited set of required ports.	Cert of compliance from Vendor
5	**Installation and Deployment**	
(a)	Proposed data security and encryption solution must support transparent deployment which does not require application code change.	To be demonstrated by vendor & checked by BOO
(b)	The proposed data protection solution must support cloud deployment with Amazon AWS, Rackspace	
(c)	The proposed data protection solution must support deployments including physical, virtual and cloud based servers with minimal administrative overhead.	
(d)	The proposed data protection solution must support a centralized policy and key management, with highly configurable security and policy enforcement to provide granular access control and audit.	
(e)	The proposed security repository must support high-availability clustering configuration across Local Area Network(LAN) and across geographies over Wide Area Network(WAN). Vendor must provide network architecture diagram to illustrate the high availability setup.	
6	**High Performance**	
(a)	The proposed data protection solution must support hardware cryptographic acceleration including • Intel and AMD AES-NI • SPARC encryption • IBM P8 cryptographic coprocessor	Cert of compliance from Govt Auth Lab/OEM
7	**Data Access Audit and Report**	
(a)	The proposed data protection solution must provide fine-grained auditing records that show system accounts and processes accessing data based on security policy.	Cert of compliance from Vendor
(b)	The proposed data protection solution must support integration with SIEM solution include: Archsight, Splunk, IBM Qradar, and deliver centralized access audit and monitoring report	

8	**Certification & Validations**	
(a)	The encryption key manager must be Common Criteria (ESM PP PM V2.1) certified	Cert of compliance from Govt Auth Lab/OEM
(b)	The encryption key manager should have option with FIPS 140-2 Level 1, FIPS 140-2 Level 2, FIPS 140-2 Level Certified	

18. EVIDENCE CENTRE

Ser No	Description of Requirements	Compliance
(a)	Ability to automatically queue multiple acquisition and processing actions – to increase efficiencies and save time	To be demonstrated by vendor & checked by BOO
(b)	End-to-end experience that brings together acquisition, processing and analysis, creating integration and a more navigable and manageable digital evidence database	
(c)	Support for a broad array of artifact types, and support for the latest versions of those apps and artifact types	
(d)	Access to file system, registry and artifacts data and trace artifact evidence to its source data efficiently for a better verification process	
(e)	The ability to present findings in a customizable way that fits their report needs and parameters.	
(f)	Acquire images from any iOS or Android device, hard drives, and removable media	
(g)	Recovers evidence from 300+ types of Internet Artifacts from Windows and Mac computers.	
(h)	Recovers 165+ types of Smartphone Artifacts from iOS, Android, and Windows Phone powered smart phones and tablets.	
(j)	Get to relevant evidence faster using filters. Isolate evidence from a specific date or time range, or create filters to narrow results based on field values for any supported artifact type. Filter stacking allows you to layer on several dimensions of filter criteria to pinpoint specific items in a large dataset.	
(k)	Create and manage a number of different tags to help you narrow down the results quickly and begin to see patterns in an individual's activity. Using the comments function, identify and share your thoughts with other key stakeholders. You can also create profiles that are associated with an individual and then associate other identifiers (email addresses, phone numbers, etc) with the profile, so that you can filter evidence to show only the evidence associated with the individual.	
(l)	Create your own custom artifact definitions to find more artifact data or have Evidence Analyzer's Dynamic App Finder automatically identify new apps and create artifact definitions which can then be saved for future use.	
(m)	recovers more artifacts from both allocated and unallocated space by extracting data from full files or carving for deleted data and traces of data elements/fragments left behind by apps and websites, presenting it in an organized and easy to read format.	
(n)	Add hash sets to either filter out non-relevant files to enhance search performance and reduce false positives or add hash sets that will specifically call out and identify known bad pictures and videos.	
(o)	Efficiently analyze large volumes of data	To be demonstrated by vendor & checked by BOO
(p)	Explore file systems and registry hives for greater insights	
(q)	Process and recover 500+ types of artifacts	
(r)	Automate all acquisition and processing tasks required to prepare evidence for analysis.	
(s)	Explore file systems and registry hives for greater insights	

(t)	Trace artifact evidence back to its source data in seconds	To be demonstrated by vendor & checked by BOO
(u)	Trace artifact evidence back to its source data in seconds.	
(v)	built on the analysis capabilities allowing you to recover hundreds of types of digital forensic artifacts	
(w)	Should be able able to extract data from cloud data source using Tokens from evidence	
(x)	Easy-to-use interface that moves you through your investigation.	

19. EVIDENCE SEIZURE KIT

Ser No	Description Of Requirements	Compliance
1	Multipurpose, Portable Unit That Contains A Complete Array Of Hardware/ Software Solutions To Preview, Acquire Or Process Digital Evidence.	To be physically checked by BOO
2	Kit Should Contain High End Forensic Laptop With The Following Minimum Configuration	
	(i). Intel Core i7-6700K Skylake Quad Core Processor, 4.0 GHz, 8MB Intel Smart Cache	
	(ii). 32 GB PC4-17000 DDR4 2133 Memory	
	(iii). 256 GB Solid State Internal SATA Drive	
	(iv). Intel Z170 Express Chipset	
	(v). 15.6" Full HD (1920x1080) IPS Display with G-Sync Technology, Matte Finish	
	(vi). NVIDIA GeForce GTX 1060 with 6 GB GDDR5 VRAM	
	(vii). 1 RJ-45 LAN (10/100/1000Mbps)	
	(viii). Intel Dual Band Wireless-AC 8260 - 802.11ac, Dual Band, 2x2 Wi-Fi + Bluetooth 4.2	
	(ix). Card Reader 6-in-1 (MMC/RSMMC/SD/Mini-SD/SDHC/SDXC up to UHS-II)	
	(x). 2.0 Megapixel FHD Video Camera	
	(xi). High Definition Audio	
	(xii). Microphone	
	(xiii). Speakers (2)	
	(xiv). 19mm Full-Size Keyboard with numeric keypad - Illuminated	
	(xv). Touch Pad pointing device(2 buttons)with multi-gesture and scrolling function	
	(xvi). Finger Print Reader	
	(xvii). 1 HDMI Port	
	(xviii). 2 Mini DisplayPort 1.3 ports	
	(xix). 1 Thunderbolt 3 / USB 3.1 Gen 2 Combo Port (Type C)	
	(xx). 1 USB 3.1 Gen 2 Port (Type C)	
	(xxi). 3 USB 3.0 ports	
	(xxii). 1 USB 2.0 Port	
	(xxiii). 1 Headphone jack (2-in-1 Heasdphone/S/PDIF Optical)	
	(xxiv). 1 Microphone jack	
	(xxv). 1 Line-In jack	
	(xxvi). 1 Line-out jack	

	(xxvii). 8 Cell Smart Lithium -Ion, 82WH Battery Pack	To be physically checked by BOO using appropriate test eqpt
	(xxviii). Kensington Lock Slot	To be physically checked by BOO
	(xxix). Universal AC Adapter (100~240V AC 50/60hz)	To be physically checked by BOO using appropriate test eqpt
	(xxx). Dimensions: 15.20 x 10.32 x 1.41 (inch)	
	(xxxi). Weight: 7.5 lbs (complete system + battery)	
	(xxxii). Windows 10 Professional (64 bit)/ Other Operating Systems included: SUSE Professional Linux (64 bit)	To be physically checked by BOO
	(xxxiii). System Restore Media - Bootable Blu-ray disc containing restore environment and factory configured operating system images	
3	KIT SHOULD CONTAIN PORTABLE FORENSIC WRITE BLOCKER WITH THE FOLLOWING INTERFACE;	
	(i). USB 3.0 - IDE/SATA, SAS, USB 3.0, Firewire, USB 3.0 Forensic Card Reader and Writer has been designed specifically for forensic use and incorporates SuperSpeed USB3 (5Gb/s) technology.	To be physically checked by BOO
	(ii). Universal Power Supply and Power Adapter cables, Standard Cables and Adapters	
4	KIT SHOUD CONTAIN LATEST FORENSIC DUPLICATOR WITH FOLLOWING CONIGURATION;	
	(i). Should have a Forensic Duplicator with capabilities to support Greater than 2TB HARD DRIVES	To be demonstrated by vendor & checked by BOO
	a. Image a 2TB HDD (2000GB)	
	b. Clone HDDs with no size limit	
	(ii). Forensically duplicates HDD 's faster than ever - up to 15 GB/min with hashing	
	(iii). Standard features include Disk-to-Disk (clone) and Disk-to-File (image) duplication, Format, Wipe, Hash (MD5 or SHA-1), HPA / DCO detection and removal, and Blank Disk Check.	
	(iv). Make one (1:1), two (1:2), or three (1:3) copies of evidence drives.	
	(v). Acquisitions of USB 3.0, SATA, and IDE/PATA devices can be directed to either USB 3.0 or SATA output devices.	
	(vi). Option to acquire SAS drives with additional modules	
	(vii). outputs to raw DD, .e01 (compressed), .ex01 (compressed), or .dmg formats	
	(viii). USB 3.0 convenience and speed built in	
	(ix). extensive log files is easy to view and save	
	(x). Built-in, user-selectable MD5 and SHA256 verification	
	(xi). Hash re-verification on read from destination(s) – user-selectable	
	(xii). Colour LCD user interface	
	EXTERNAL DEVICES AND ENCLOSURES	
	(i). USB3 Read Only/Read Write switchable External Hard Drive Chassis with Power Supply	
	(ii). Digital Intelligence Integrated Forensic Media Card Reader - Read-Only and Read/Write Switchable	

	EXTRAS	
	(i). Hard Drive Adapter 2.5 Inch	To be physically checked by BOO using appropriate test eqpt
	(ii). Hard Drive Adapter 1.8 Inch	
	(iii). TDA5-ZIF ZIF HD Adapter w/case	To be physically checked by BOO
	(iv). TDA3-1 Micro SATA HD Adapter	
	(v). SATA LIF Adapter	
	(vi). Blade Type SSD Adapter	
	(vii). FireWire Adapter 9pin to 4pin	
	(viii). FireWire Adapter 9pin to 6pin	
	(ix). Micro/Mini SD to SD Adaptor Kit	
	(x). 2 TB SATA Hard Drive	
	(xi). Precision Electronic Tool Kit	
	(xii). Power Strip - 120v/240v Compatible	
	(xiii). Universal Power Adapter	
5	PELICAN CASE	
	(i). Hard-sided with Padded Laptop Insert	To be physically checked by BOO
	(ii). Watertight / Airtight	
	(iii). High Impact	
	(iv). Custom Foam Lined	
	(v). Custom Lid Organizer for Cables and Adapters	
	(vi). 24" x 20" x 14" - 58lbs	To be physically checked by BOO using appropriate test eqpt
6	SOFTWARE	
	(i). Microsoft Windows 98SE Standalone DOS (Configured & Pre-Installed)	To be physically checked by BOO
	(ii). Microsoft Windows 8 Professional 64 bit (Configured & Pre-Installed)	
	(iii). Microsoft Office 2016	
	(iv). Suse Linux Professional (Pre-Configured)	
	(v). Symantec GHOST	
	(vi). DVD/CD Authoring Software	
	(vii). High-End Forensic laptop should come pre-installed with Forensic analysis software with Live Boot virtualization, Shadow Copy, Meta extraction, Carving, Hash Sets, Index and Keyword search, flexible graphic user interface (GUI) with advanced sorting, filtering, keyword searching, previewing and scripting technology and Bookmarking capability. The	

	software should allow the investigator to Boot forensic image files and view electronic evidence in a forensically sound virtual environment. Boot both Windows (all versions) and Macintosh computers.	To be physically checked by BOO
	Product Offered should be of International Repute & Brand and should not be assembled Machine.	Cert of compliance from Vendor
	(viii). In case of Distributor/ Reseller; OEM/ Manufacturer's Authorization for Supply and Service should be attached with the Tender.	
	(ix). Bidder should have OEM trained Manpower for Product Installation and support, Supporting document for the same to be attached.	

20. INTELLIGENT INVESTIGATION MANAGEMENT SYSTEM

Ser No.	Specification	Compliance
1	Tool should be collaborative end-to-end product that uses a clean, intuitive interface, allowing anyone get started with very little training. It should provide digital evidence and lab management, as well as archiving, which allows teams to understand how the evidence was handled and where to find it in the future.	To be demonstrated by vendor & checked by BOO
2	Tool should works through common browsers on Windows, Mac, Linux, and mobile OSes and it builds statistics as you enter information. It should be able to incorporate case management stats into reporting tools.	
3	Also have below features:	
(a)	Global Collaboration on Any Case	
(b)	Unlimited Client Base	
(c)	Permanent Case Archives	
(d)	Chain of Custody Preservation	
(e)	Complete Exam Documentation	
(f)	Curriculum Vitae Management	
(g)	Asset Management	
(h)	Local or Remote Browser Access	
(j)	Consolidation of All Case Information	
(k)	Automatic Statistics Generation	
(l)	ICAC and Cybertip Management for Law Enforcement	
(m)	Financial Information Management	
(n)	Lab Expenses Analysis	
(o)	Grant Documentation Management	
(p)	Project Expense Accountability	
(q)	Invoice Generation	
(r)	Process Review Facilitation	
(s)	In- eld Evidence Triage	
(t)	Scalability to Grow with Your Needs	
(u)	Barcode Generation	
(v)	Secure 256-bit Encryption	Cert of compliance from Govt Auth Lab/ OEM
(w)	Standardized, repeatable process management	Cert of compliance from Vendor

21. SECURITY MODULE

Ser No	Required Technical Specification	Compliance
Functional Capabilities		
(a)	Must support cryptographic offloading and acceleration	To be demonstrated by vendor & checked by BOO
(b)	Should provide Authenticated multi-level access control	
(c)	Must have strong separation of administration and operator roles	
(d)	Capability to support client authentication	
(e)	Must have secure key wrapping, backup, replication and recovery	
(f)	Must support unlimited protected key storage	
(g)	Must support clustering and load balancing	
(h)	Should support Logical cryptographic separation of application keys	
(j)	Must support —k of nǁ multi-factor authentication	
Application Program Interfaces (APIs)		
(a)	PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI and CNG	Cert of compliance from Vendor
Host connectivity.		
(a)	Dual Gigabit Ethernet ports (to service two network segments)	To be physically checked by BOO
Cryptography		
(a)	Asymmetric public key algorithms: RSA, Diffie-Hellman, DSA, KCDSA, ECDSA, ECDH	Cert of compliance from Govt Auth Lab/OEM
(b)	Symmetric algorithms: AES, ARIA, Camellia, CAST, RIPEMD160, HMAC, SEED, Triple DES	
(c)	Hash/message digest: SHA-1, SHA-2 (224, 256, 384, 512 bit)	
(d)	Full Suite B implementation with fully licensed ECC including Brainpool and custom curves	
Security compliance		
(a)	FIPS 140-2 Level 3	Cert of compliance from Govt Auth Lab/OEM
Safety and environmental compliance		
(a)	Compliance to UL, CE, FCC part 15 (for Commercial products)	Cert of compliance from Vendor
(b)	Compliance to RoHS2, WEEE	
Management and monitoring		
(a)	Support Remote Administration —including adding applications, updating firmware, and checking the status— from NoC	To be demonstrated by vendor & checked by BOO
(b)	Syslog diagnostics support	
(c)	Command line interface (CLI)/graphical user interface (GUI)	
(d)	Support SNMP monitoring agent	
Physical characteristics		
(a)	Standard 1U 19in. rack mount with integrated Smart Card Reader	To be physically checked by BOO using appropriate test eqpt
Performance		
(a)	RSA 2048 bit signing performance 3,000/second and RSA 2048 key generation performance min 10 keys/second	Cert of compliance from Vendor
(b)	ECC 256 bit prime curve signing performance 5000 /sec and ECC 256 bit key generation performance - 800/sec	
Custom Application		
(a)	Should enable secure execution of custom security-critical application code within the tamper resistant hardware boundary	Cert of compliance from Vendor

Key Generation and Protection		
(a)	Ability to generate RSA keys (2048 and 4096) on board on demand and shall be secured by high security module in accordance with FIPS 140-2 level 3 recommendations for Cryptographic Modules Validation.	Cert of compliance from Govt Auth Lab/OEM
Key back up and restoration		
(a)	The proposed solution must include the software/hardware to - securely store the keys at DC, at DR and at one remote location and restore them in case of necessity	To be physically checked by BOO using appropriate test eqpt
No. of Keys to be protected		
(a)	The HSM must secure a minimum of 1 lakh keys in accordance with FIPS 140-2 level 3 standards. The licensing and HSM hardware must have no restriction on the number of keys to be protected	Cert of compliance from Vendor
Performance upgrade of HSM		
(a)	The performance of HSM should be upgradable on field.	Cert of compliance from Vendor
Instant Key reflection		
(a)	Multiple HSMs to be supportable for DR, key backup, key update, and key processes, load balancing and failover. Should support instant key reflection to all the HSMs in the system.	Cert of compliance from Vendor
Logical partitions		
(a)	Unlimited logical/cryptographic separation of application keys. all The licenses must be included	Cert of compliance from Vendor

22. TIME SERVER

Ser No	**Description of Requirements**		**Compliance**
	Power Supply:		
1	Voltage	230 +/- 10% V AC	To be physically checked by BOO using appropriate test eqpt
2	Frequency	47-55 Hz	
	Functions/ Features :		
3	Time Facility	Using Universal Time co-ordination(UTC)	To be physically checked by BOO
4	Propagation delay Compensation	Supported	Cert of compliance from Vendor
5	Accuracy	# +/- 250 Nanosecond	To be physically checked by BOO using appropriate test eqpt
6	Time Accuracy	Better than 1 PPM	
7	LCD Display	Front panel LCD display to show status, time and no. of satellites	To be physically checked by BOO
8	**Inputs**	GPS Antenna input through BNC connector.	
9		Power Supply	
	Outputs		
10	NTP output (2 nos. customizable) for NTP client access through RJ-45 .Both Ports shall be independent		

11	RS232 serial port output (2 Nos)		To be physically checked by BOO
12	Pulse output: 1 PPS, ½PPM, 1PPM (Configurable).		
13	Support Client request per Second	10,000	To be physically checked by BOO using appropriate test eqpt
	Antenna		
14	Length of GPS	50 meters	To be physically checked by BOO using appropriate test eqpt
15	Gain	Over 30 DB	
16	RECEIVER,GLOBAL POSITIONING SYSTEM,DISPLAY TYPE:LCD;DISPLAY SIZE:2 X 3.5 INCH;DISPLAY RESOLUTION:240X400 PIXELS;DATA INTERFACE:ETHERNET;PC INTERFACE:ETHERNET;;EXPANSION SLOT TYPE:USB;WAY POINTS:2; Server FREQUENCY:48-55 HZ; OPERATING TEMPERATURE:0-55 DEG.C;ELECTRICAL RATING:230 VAC;ADDITIONAL INFORMATION:WITH ANTENNA and Surge Arrestor		

Tele : 0364-2705101
Fax : 0364-2230146
e-mail:hqdgar@hotmail.com

Mahanideshalaya Assam Rifles
Direcotorate General Assam Rifles
Shillong – 793010

XX.11011/23/IT (Proc)/2018-Sigs/128

13 Jul 2018

Ministry of Home Affairs
Directorate General Central Reserve Police Force
East Block-7, Sect-1
R.K. Puram,
New Delhi – 110066
Email:- comncell@crpf.gov.in

DRAFT TRIAL DIRECTIVE (TDs) IN RESPECT OF CYBER SECURITY MONITORING CENTRE

1. Please ref your letter No B.V-7/2018-19-C(QRs) dt 10 Jul 2018.

2. Draft trial Directives (TDs) in respect of Cyber Monitoring Centre are forwarded herewith for necessary action please.

Sd/-xx xx xx
(Ashish Negi)
Lt Col
SO1(IT & Comn)
for Chief Signal Officer

Encl: As above