EXPRESSION OF INTEREST/INFORMATION (EOI) FOR

DEPLOYMENT OF ENTERPRISE GRADE END POINT PROTECTION SOLUTION FOR INDIAN NAVY WITH ONSITE SUPPORT FOR A PERIOD OF THREE YEARS

IT/0622/14 DATED 10 Oct 16

1. The Directorate of Information Technology, Integrated Headquarters Ministry of Defence (Navy) intends to procure enterprise grade End Point Protection (EPP) solution to expand the functions of Security Operations Centre (SOC) and exercise stringent control over all end point machines.

2. This Expression of Interest (EOI) (Refer Para 4.8.1 of DPM-09) consists of two parts as indicated below:-

(a) **Part I**. The first part of the EOI incorporates functional and technical requirements for enterprise end point security that should be met by the solution. A few important technical parameters of the proposed solution are also mentioned.

(b) **Part II**. The second part of the EOI states the methodology of seeking response of vendors.

Part I

Background

3. Indian Navy has been at the forefront for developing and deploying security software in order to ensure protection of data on naval networks. Since ingress/ egress of information cannot be centralised, Indian Navy is looking for a solution to control and monitor use of portable storage devices, monitor information flow through portable storage devices and apply centralised file transfer policies.

4. With increased network penetration and the requirement to centralise management, Indian Navy is looking for a state of the art enterprise grade endpoint port and device control software meeting the highest industry standards.

Important Technical Requirements.

5. Indian Navy has an internal network that is physically and logically air gapped from internet. This network spans the entire country.

6. The proposed system will be implemented for all Naval computers. The overall population may range from 25000 to 40000 machines.

7. The proposed system should support federated/ multi level management so that end point devices can be registered and managed at multiple locations.

Therefore, preferred licensing mechanism would be per device based licences rather than server side licensing.

8. The system should also support role based access control which can be applied to groups. For example, it should be possible to assign a set of users and computers to a group and assign the group to be managed by an administrator.

9. Broad technical requirements envisaged at this stage are placed at Appendix A. In your response, please indicate whether the offered solution fulfills the above requirement (serially). However, these requirements are only generic in nature and do not put any limitation on the technical specifications of the final product.

10. The firm should also answer the questionnaire placed at Appendix B.

11. Include any additional details/ features of the solution being proposed, to bring out features, functions and industry standards.

12. The vendor is to provide following additional inputs:-

(a) **Approximate Cost Estimate**. Indicative cost for setting of enterprise end point protection solution in *IN*. It should take into account all aspects of supply, installation, integration, training, life cycle support. The indicative cost should also cater to the solution support as per details for three years. Other aspects (if any), may be mentioned specifically.

(b) Vendor is to indicate whether he has supplied the same or similar solution to any other customer. Additionally, the vendor is to indicate whether similar solution is in use in by any other defense establishment.

(c) Vendor is to indicate the manpower required to operate and maintain the solution. Additionally, the details of training required for such personnel are also to be indicated.

(d) Vendors may consider EOI as advance information to obtain requisite Government clearances.

(e) **Tentative Delivery Schedule**. The overall timeframe of delivery and installation with stage wise break-up of the entire project post conclusion of contract is required to be submitted.

(f) **Payment Terms**. Vendor is to indicate acceptability to the terms of payment as per DPM-2009.

(g) Vendor is to indicate its capability to execute the project and provide product support including technical solution support and update.

(h) Vendor is to indicate the provisions for upgradeability of solution to avoid system obsolesce.

(j) Earliest date by which OEM/Vendor is willing to give a presentation at Naval Headquarters, New Delhi.

13. Vendor should confirm that the following conditions are acceptable:-

(a) The solicitation of offers will be as per '**Single Stage –Two Bid System'**. It would imply that a '**Request for Proposal'** would be issued soliciting the technical and commercial offers together, but in two separate sealed envelopes. The validity of commercial offers would be at least 06 months from the date of submission of offers.

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

(c) Amongst the vendors cleared by TEC, a Commercial Negotiation Committee (CNC) would decide the lowest cost bidder (L1) and conclude the appropriate contract.

(d) Vendor would be bound to provide product support for time period specified in the RFP, which includes solution support.

(e) Vendor is to accept all conditions of DPM-09, if not, which Para/ Clause of DPM-09 is not acceptable is to be indicated.

Part II

14. **Procedure for Response**

(a) Vendor must fill the form of response as given in Appendix C. Apart from filling details about the company, details about the exact product meeting the generic technical specifications should also be carefully filled. Additional literature on the product may be attached with the form. Vendors are to provide para wise compliance in a tabular format to this EOI along with reasons for non-compliance, if any to all aspects of this EOI.

(b) The filled form should be dispatched at under mentioned address:-

Principal Director of Information Technology
Directorate of Information Technology
IHQ MoD(Navy)
Room No. 129, 'C' wing Sena Bhawan
New Delhi – 110 010

Tel: +91-11-23011517
Fax No.: +91-11- 23010612
E-mail: mandeep@navy.gov.in

(c) The last date of acceptance of filled form is **28 Nov 16**. A presentation on the subject may also be sought in case it is felt that certain parameters mentioned in replies to this EOI need further clarification.

15. The Indian Navy invites responses to this request only from Original Solution Manufacturers (OEM) / Authorised Vendors. The end user of the solution is the Indian Navy.

16. This information is being issued with no financial commitment and the Indian Navy reserves the right to change or vary any part thereof at any stage. The Government of India also reserves the right to withdraw it should it be so necessary at any stage.

(xx—sd—xx)
(Akshay Chuloo)
Commander
Joint Director (IT)

Appendix A

FUNCTIONAL AND TECHNICAL REQUIREMENTS FOR ENTERPRISE GRADE END POINT PROTECTION SOFTWARE FOR INDIAN NAVY

1. Endpoint Protection (EPP) Software shall provide for following:-

   (a) Control use of all USB and other storage devices.
   (b) Tracking of data saved to storage devices.
   (c) Tracking of data that is copied from and to storage devices
   (d) Scanning of all data transfers for sensitive content detection.
   (e) Complete monitoring/blocking of all possible data exit points.
   (f) Authorize the use of USB storage devices
   (g) Securing data on USB storage devices (Encryption of drive/data).
   (h) Powerful reporting tool and audit

2. EPP shall be modular and provide a centralised web based device management and dashboard.

3. EPP should enable network administrators to centrally monitor and report what data is introduced into the corporate network from a portable storage device such as prohibited materials (MP3s, movies or games) or harmful data like a virus that could jeopardize the networks integrity.

4. EPP shall allow authorised use of certain device types or specific devices such as Indian Navy's own USB Flash Drives to handle and transfer confidential data. These devices should be able to be mapped to certain user(s), groups of users, specific computer(s) or groups of computers.

5. To ensure the protection of data carried by users on authorized devices, the EPP administrator should be able to enforce copy work data only to a password protected / encrypted area of an authorized device, a so called "Trusted Device"

6. EPP shall have the option to offer full-disk and file encryption, encryption key management, endpoint DLP, and extremely granular device control.

7. EPP must be able to upgrade seamlessly from previous versions in future.

8. EPP must have mechanisms to monitor the health of installed agents and alert the Administrator if an agent was deactivated?

9. EPP must have a minimal footprint on the client computers and cause little to no impedance in the client's performance.

10. EPP should be able to scan and report all transfers of sensitive data on and from any removable media including comparison with ‘Dirty’/Alerted Word List.

11. EPP should support File Whitelist and Blacklist in that it should allow only previously authorized files to be copied to portable storage devices.

12. EPP should provide Group-based protection control – EPP should be able to configure and place computers into groups that are governed by one protection policy. It should allow Administrator to configure a single protection policy and apply it to all the computers that are members of that group. It should be able to integrate and read groups from the Active Directory.

13. EPP should provide granular access control – EPP should enable Administrator to allow or deny access to a specific device as well as to assign (where applicable) ‘full’ or ‘read only’ privileges over every supported device (e.g.CD/ DVD drives, PDAs) on a user by user basis.

14. Scheduled deployment – EPP should allow scheduling the deployment of protection policies and any related configuration changes without the need to manually do it from the management console. The deployment feature should also be able to handle failed deployments through automatic rescheduling.

15. EPP should provide automatic discovery of PCs without agent and deploy agents on them. EPP may use Indian Navy’s Active Directory services or the SCCM services for the same.

16. EPP must support device activity logs for all clients and devices connected.

17. Naval Intranet has a single forest multiple domain architecture with many OU Admins managing their own users and computers. EPP should allow deployment in a distributed architecture with each OU Admin having rights to register devices and create policies for the users and computers in his control. However, live logs (when network is available) must be forwarded to central servers so that a complete picture is available to the Navy SOC at all times. It should be possible to generate reports based on navy wide data. It should also be possible to sync log data from various implementations into central servers as per defined intervals.

18. EPP should be able to integrate with HP Arcsight SIEM for log forwarding or to Windows Event Manager. In case the EPP is able to write events into the Windows Event Manager or forward it directly to SIEM, then the requirement of log centralisation within the EPP solution does not exist.

19. The EPP should be able to integrate with **existing Active Directory for reading Users, Computers and Groups and apply group policies on them**. EPP should also **support automatic AD synchronisation** to ensure data is always current.

20. The EPP should be able to report filenames being transferred along with the full path of the file including From and To paths. This should be applicable whether the file is being transferred from/ to storage device or across network file shares. For some files marked as important, EPP should provide file shadowing feature wherein a copy of the transferred file is saved in the system for audit purposes.

21. The EPP agent deployed on machines should have inbuilt tamper protection. Users should not be able to remove agents/change any settings.

22. EPP should provide facility for offline Patch Management/ Upgrade since Naval networks are air gapped from Internet.

23. For units deployed with thin clients, EPP should support Terminal Server Management (RDP Storage) so that thin clients can legitimately use storage on servers.

24. EPP shall support Content Awareness and File Shadowing. This should be configurable by the Administrator.

25. EPP shall support and provide implementation of following deployment scenarios:-

(a) Bind a device to a user/ group of users.

(b) Bind a device to a computer/ group of computers.

(c) Bind a device class to a/ group of users or computers.

(d) Allow Read Only or Read Write privileges.

26. EPP should preferably have a Web based interface.

27. EPP shall provide the following Access control –

(a) Block a range of device categories such as Floppy drive, CD drive etc.

(b) By file type -for example, allow the user to read *.doc files but block access to all *.exe files.

(c) By physical port -all devices connected to particular physical ports, for example, all devices connected to USB ports.

(d) By device ID - block access to a single device based on the unique Hardware ID of the device.

28. EPP must support Device whitelist and blacklist - The administrator can define a list of specific devices that are permanently allowed and others that are permanently banned.

29. Temporary access - The administrator is able to grant temporary access to a device (or group of devices) on a particular computer. This feature allows the administrator to generate an unlock code that the end-user can use to obtain a time-limited access to a particular device or port, even when the EPP agent is not connected to the network.

30. Deployment through MSI – The EPP shall support automatic deployment of agents through Active Directory group policy or Microsoft SCCM. This needs the agent to be available in MSI format.

31. Device discovery - The EPP should be able to scan and detect the presence of devices on the network, even on computers that are not assigned any protection policy. The information gathered about detected devices can then be used to build security policies and assign access rights for specific devices.

32. Alerting – The EPP shall support e-mail alerts and network messages that can be sent to specified recipients when devices are connected or disconnected, when device access is allowed or blocked and upon service generated events.

33. EPP shall support Custom messages - When users are blocked from using devices, they are shown popup messages explaining the reasons why the device was blocked.

34. Device encryption - For maximum security, EPP must provide for encryption of storage devices using AES 256 encryption. Encryption must be enforceable on specific computers running agents over the network.

35. The solution should support full disk/ file level encryption for removable devices in such a manner that encrypted files are accessible from either connected PCs on the network or physically disconnected machines outside the network.

36. The solution shall support password recovery for encrypted removable disk.

37. Removable disks, protected by the EPP, whether encrypted or otherwise, should be readable by variety of platform, including but not limited to Windows and Debian Linux.

38. Content awareness - The content awareness feature of EPP should enable users to look into files entering the endpoints via removable Devices. Content should be identified based on predefined (or custom) regular expressions and dictionary files.

39. EPP shall support the following device categories:-

(a) Removable Storage Devices such as USB Flash Drives, U3 and Autorun Drives, Disk on Key, etc.

(b) LPT/Parallel ports

(c) Floppy disk drives

(d) Memory Cards - SD Cards, MMC Cards, and Compact Flash Cards, etc.

(e) Card Readers - internal and external

(f) CD/DVD-Player/Burner - internal and external

(g) Smartphones/ Tablets etc.

(h) MP3 Player / Media Player Devices

(j) External HDDs/ portable hard disks

(k) FireWire Devices

(l) PCMCIA Devices

(m) Biometric Devices

(n) Bluetooth

(p) Printers - Applies to serial, USB and LPT connection methods

(q) ExpressCard (SSD)

(r) Network Adapters, including: Ethernet adapters, Wi-Fi adapters, Removable adapters (USB, Firewire, PCMCIA) etc.

(s) Modems, including: Smart-phones Mobile phones

(t) Imaging Devices: Digital cameras Webcams Scanners

(u) Human Interface Devices: Keyboards Mice Game controllers

(v) Other Devices: Bluetooth dongles/ports Infrared dongles/ports Zip drives Tape drives MO (magneto optical) drives (internal and external)

40. The EPP shall support control of following connectivity ports:-

(a) USB

(b) Secure Digital (SD)

(c) Firewire

(d) Bluetooth

(e) Infrared

(f) PCMCIA

(g) Serial & Parallel

(h) Internal (example: optical drives connected internally on PCI)

Appendix B

PRODUCT QUESTIONNAIRE

1. Explain how your software updates definitions work for your EPP solution.

2. On the table below, list all updates released for the month of July 2016 or the latest update, including the version, file(s) size, date and time of the release in the table provided. (Use additional space as needed).

Version	File(s)	Size	Date	Time

3. The software must be capable of being updated from multiple locations including, but not limited to the EPP's Internet source(s) and from our own network. Explain how updates may be installed from both our wide area network, as well as the vendor Internet repository. List the physical locations of available update sites.

4. The EPP requires central management of all installations with distributed management available to individual agencies via a secure interface, and the ability to install and/or update from remote locations. Provide details on how this is accomplished with your product.

5. Describe the process for creating custom distribution packages providing the ability to change update times and locations, scan settings, etc.

6. The software solution must have an unalterable base policy configuration. Describe the granularity of administration for rights in a hierarchal, distributed management environment.

7. Describe how the agents communicate with server components.

8. The solution must have small resource (CPU/memory) utilization. Describe the ability of your software to keep resource use to a minimum.

9. How much disk space is required?

10. How much memory is consumed under normal conditions? During scans?

11. What is the CPU usage under normal conditions? During scans?

12. Can administrators adjust the foot print and/or CPU usage manually or via a policy?

13. Are there any known conflicts with other applications or services?

14. Does the client process shut down after a predetermined amount of time?

15. Describe how the client reports back to the server.

16. Does the client operate as an application or a service? Explain fully.

17. If the client operates as an application, what local workstation rights are required to perform scans, updates and cleans? Explain in detail.

18. If the client operates as a service, what local workstation rights are required to perform scans, updates and cleans? Explain fully.

19. At what point in the boot process does the product start? Describe in detail.

20. Describe modes of operation: user interactive, user alerting only, silent, other

21. Describe the control system administrators have over the end-user's ability to make any changes to settings.

22. Detail your product's ability to send logging information to a remote server for event correlation.

23. Describe your software's ability to create centralized and distributed, ad hoc and scheduled reports of up-to-date, as well as out-of-date devices.

24. Describe your program's ability to notify system administrators of significant events via e-mail, network messaging, or similar notification mechanisms and the ability to customize this function.

25. Describe your EPP device control process and how does it differentiate with those of your competitors?

26. EPP needs to have the capability to detect new end points that join the network that do not already have your client installed. How is this achieved in your solution?

27. What is the typical ratio of management servers to clients in practice, and what factors affect this ratio?

28. Explain how the management server pushes updates and pulls status info of clients that are part of domain, in workgroups outside domain but on same network and standalone clients.

29. Is it possible for EPP to create a new group of clients in the management console that is not an Active Directory group and report on that new group or use this group in policy? YES or NO.

30. List the agents that must be installed on the client for the full EPP functionality.

31. Does the solution allow event/log data to be sent to a SIEM solution, specifically HP ArcSight? YES or NO.

32. Can the backend server and database run within a totally virtual environment? YES or NO.

Appendix C

INFORMATION PROFORMA (VENDORS)

1. **Name of the Vendor/Company/Firm**.

_____

_____

(Company profile, in brief, to be attached)

2. **Type (Tick the relevant category)**.

Original Solution Manufacturer (OEM):- Yes/No

Authorised Vendor of foreign Firm:- Yes/No (attach details, if yes)

Others (give specific details) _____

3. **Contact Details**.

Postal Address: - _____

City: _____State: _____

Pin Code: _____Tele: _____

Fax: _____URL/Web Site: _____

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

Name & Address: _____

Pin code: _____Tel: _____Fax: _____

5. **Financial Details.**

(a) Category of Industry (Large/medium/small Scale):_____

(b) Annual turnover: ___(in INR)

(c) Number of employees in firm: ___

(d) Details of manufacturing infrastructure:-

_____

(e) Earlier contracts with Indian Ministry of Defence /Government agencies:

Contract Number	**Solution**	**Quantity**	**Cost**

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

Name of Agency	**Certification**	**Applicable from (date & Year)**	**Valid till (date & year)**

7. **Details of Registration**

Agency	Registration No	Validity (Date)	Solution
DGS&D			
DGQA/DGAQA/DGNAI			
OFB			
DRDO			
Any other Government Agency			

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

Name of Organization	Membership Number

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

(a) Name of Product : _____

(IDDM Capability to be indicated against the product)

(Should be given category wise for eg. All products under night vision devices to be mentioned together)

(b) Description (attach technical literature): _____

(c) Whether OEM or Integrator : _____

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

(e) Industrial License Number: _____

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

(g) Status (in service /design & development stage): _____

(h) Countries/agencies where solution supplied earlier (give details of quantity supplied):_____

(j) Estimated price of the solution _____

10. Alternatives for meeting the objectives of the solution set forth in the EOI.

11. Any other relevant information:_____

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

(Authorised Signatory)