SECURITIES AND EXCHANGE COMMISSION OF PAKISTAN

CORRIGENDUM

Reference to SECP Invitation to bid **(Tender No. 24/19-20)** published in newspapers (Dunia and Business Recorder) on January 02, 2020 for **"Supply, Installation and Configuration of Data Loss Prevention (DLP) solution / Supply, Installation and Configuration of Enterprise Mobility Management (EMM) solution.".**

It is informed that due to change in the requirement the last date for submission of bids for the said requirement has been extended from January 21, 2020 to February 03, 2020.

Revised bidding documents containing detailed terms and conditions, method of procurement, procedure for submission of bids, bid bond/security, bid validity, opening of bid, evaluation criteria, clarification/rejection of bids etc. against above requirement are available for the interested bidders from the undersigned free of cost and can also be downloaded from https://www.secp.gov.pk/procurement/

The bids prepared in accordance with the instructions in the bidding documents, must reach undersigned on or before **February 03, 2020** by 1030Hrs and will be opened on the same day at 1100Hrs.

In case of any query, Admin Department may be contacted on Telephone No. 051-9207091-4 (Ext-437/444) during office hours (Monday to Friday excluding Public Holidays)

Deputy Director (Admin)

Advertisements/Tender Notices Published on January 02, 2020

Business Recorder
Thursday, January 2, 2020

Securities and Exchange Commission of Pakistan
NICL Building, Jinnah Avenue, Islamabad

T# 24/19-20

INVITATION TO BID

The Securities & Exchange Commission of Pakistan invites sealed bids from the suppliers based in Pakistan and registered with Federal Board of Revenue/Respective Revenue Boards for Income Tax and Sales Tax and who are on Active Taxpayers List (Income and Sales tax) of the Federal Board of Revenue/Relevant Tax Authority for

Supply, Installation and Configuration of Data Loss Prevention (DLP) Solution /Supply, Installation and Configuration of Enterprise Mobility Management (EMM) Solution.

Bidding documents containing detailed terms and conditions, method of procurement, procedure for submission of bids, bid bond/security, bid validity, opening of bid, evaluation criteria, clarification/rejection of bids etc. against above requirement are available for the interested bidders from the undersigned free of cost and can also be downloaded from https://www.secp.gov.pk/procurement/

The bids prepared in accordance with the instructions in the bidding documents, must reach undersigned on or before **January 21, 2020 by 1030 Hrs** and will be opened on the same day at **1100 Hrs.**

In case of any query, Admin Department may be contacted on Telephone No. 051-9207091-4 (Ext-437/444) during office hours (Monday to Friday excluding Public Holidays)

Deputy Director (Admin)
NICL Building, 63 Jinnah Avenue, Blue Area Islamabad
"SAY NO TO DRUGS"

PID(I)3571/19

روزنامہ دنیا
Thursday, January 2, 2020

سیکیورٹیز اینڈ ایکسچینج کمیشن آف پاکستان

ٹینڈر نمبر 24/19-20

پیشکشوں کی طلبی

سیکیورٹیز اینڈ ایکسچینج کمیشن آف پاکستان (ایس ای سی پی) کو انکم ٹیکس اور سیلز ٹیکس کیلئے فیڈرل بورڈ آف ریونیو/متعلقہ ریونیو بورڈز کے ساتھ رجسٹرڈ اور فیڈرل بورڈ آف ریونیو/متعلقہ ٹیکس اتھارٹی کی فعال ٹیکس پیئر لسٹ (انکم اور سیلز ٹیکس) پر موجود، پاکستان میں قائم سپلائرز سے سربمہر پیشکشیں مطلوب ہیں۔

Supply, Installation and Configuration of Data Loss Prevention (DLP) Solution / Supply, Installation and Configuration of Enterprise Mobility Management (EMM) Solution.

تفصیلی شرائط وضوابط، پروکیورمنٹ کا طریقہ کار، پیشکشیں جمع کرانے کا طریقہ، بڈ بانڈ/سکیورٹی، بولی کی موثریت، پیشکش کا کھلنا، ایوالوایشن کا معیار، پیشکشوں کی وضاحت/مسترد وغیرہ پر مشتمل درج بالا کے مطابق بولی دستاویزات خواہشمند بولی دہندگان کیلئے زیرِ تحفظی کے پاس بلا معاوضہ دستیاب ہیں اور https://www.secp.gov.pk/procurement/ سے بھی ڈاؤن لوڈ کی جاسکتی ہیں۔

بولی دستاویزات میں درج ہدایات کے مطابق تیار کردہ پیشکشیں **21 جنوری، 2020** صبح **10:30** بجے تک زیرِ تحفظی کو پہنچ جانی چاہئیں جو اسی دن صبح **1100** بجے کھولی جائیں گی۔

کسی بھی استفسار کی صورت میں، ایڈمن ڈیپارٹمنٹ سے ٹیلیفون نمبر 051-9207091-4 (ایکسٹینشن 437/444) پر دفتری اوقات کے دوران (پیر تا جمعہ ماسوائے عام تعطیل) رابطہ کیا جاسکتا ہے۔

ڈپٹی ڈائریکٹر (ایڈمن)
ایس ای سی پی بلڈنگ، 63 جناح ایونیو، بلیو ایریا، اسلام آباد
"منشیات سے انکار زندگی سے پیار"

PID(I)3571/19

Terms and Conditions for Bids and Bidders

1. Tender Identification Number: **TENDER # 24/19-20**

The Procurement Agency is:

Securities and Exchange Commission of Pakistan
4th Floor, NICL Building, 63 Jinnah Avenue, Blue Area,
Islamabad.

2. The Securities and Exchange Commission of Pakistan invites sealed bids from suppliers based in Pakistan and registered with Federal Board of Revenue/Respective Revenue Boards for Income Tax and Sales Tax and who are on Active Taxpayers List (Income and Sales tax) of the Federal Board of Revenue/Relevant Tax Authority for

Supply, Installaion and Configuration of Data Loss Prevention (DLP) solution /
Supply, Installaion and Configuration of Enterprise Mobility Management (EMM) solution.

through

SINGLE STAGE TWO ENVELOP METHOD

3. Bidder may submit its bid against any one of the required functionalities/solutions i.e. either for Supply, Installaion and Configuration of Data Loss Prevention (DLP) **OR** for Supply, Installaion and Configuration of Enterprise Mobility Management (EMM) solution.

4. **Clarification** if any on the technical requirement may also be obtained by sending an email at ubaidullah.khalid@secp.gov.pk.

5. Bid shall comprise a single package containing TWO separate envelopes. Each envelope shall contain separately the financial Bid and the technical Bid. The envelopes shall be clearly marked as **"FINANCIAL BID"** and **"TECHNICAL BID"** in bold and legible letters.

6. The Bid Bond to be enclosed in a **SEPARATE ENVELOPE**, labelled as **"BID BOND",** and should be **SEALED** and enclosed in the main envelop.

7. BID Bond should not be ENCLOSED in the envelope of financial OR technical proposal.

8. Initially, only the envelope marked **"TECHNICAL BID"** shall be opened publicly. The envelope marked as **"FINANCIAL BID"** shall be retained.

9. After the evaluation and approval of the technical bid, financial bids of the technically accepted bids only will be opened at a time, date and venue announced and communicated to the bidders in advance. Financial bids of technically unsuccessful bidders will be returned.

10. The amount of the bid and bid bond/security shall be in Pak rupees. The bids should be accompanied by bid bond/security (refundable) for an amount equal to 2% of the total quoted price (inclusive GST, if applicable) in shape of either pay order, demand draft valid for not less than 6 months in favor of Securities and Exchange Commission of Pakistan.

11. Bids not accompanied by bid bond/security or with less amount of bid bond/security will not be entertained.

12. In case any bidder submits more than one option against this invitation then bid bond/security shall be submitted against highest quoted option.

13. Only registered suppliers who are on Active Taxpayers List (ATL) of FBR are eligible to supply goods/services to the Commission. **Bids of all those bidders not found on ATL shall be rejected.**

14. If any supplier is not in ATL at the time of payment then his payment shall be stopped till he files his mandatory returns and appears on ATL of FBR.

15. Tax shall be deducted/withheld as per applicable sales tax and income tax law.

16. Relevant details plus terms and conditions of the invitation may be obtained from the undersigned personally or by visiting the SECP website: https://www.secp.gov.pk/procurement/

17. SECP reserves the right to cancel this invitation and reject all bids at any stage of the bidding process.

18. The bid validity period shall be 150 days.

19. If the bid is withdrawn after bid opening time and before the expiry of bid validity the bid bond/security will be forfeited in favor of the SECP, Islamabad.

20. The language of the bid is English and alternative bids shall not be considered.

21. Amendments or alterations/cutting etc., in the bids must be attested in full by the person who has signed the bids.

22. The prices quoted shall correspond to 100% of the requirements specified. The prices quoted by the bidder shall not be adjustable. Changes or revisions in rates after the opening of the bids will not be entertained and may disqualify the original offer.

23. The rates must be quoted strictly in accordance with our documents and Annex(s).

24. Discounts (if any) offered by the bidder shall be part of the bid and for taxation purposes will be treated in accordance with the applicable laws.

25. Detail of applicable taxes and whether taxes included or not in the quoted price and breakup of the quoted price shall be clearly mentioned.

26. The bidder shall be responsible for payment of any duties/taxes etc. which are imposed by the Government of Pakistan (GOP). The bided price MUST be inclusive of all applicable taxes.

27. The bidder is hereby informed that the Commission shall deduct tax at the rate prescribed under the tax laws of Pakistan from all payments for supply/services rendered by any responding organization who accepts the Purchase order or signs agreement with the Commission.

28. In case applicable taxes have neither been included in the quoted price nor mentioned whether quoted amount is inclusive or exclusive of such taxes, then quoted amount will be considered inclusive of all taxes.

29. Selected service provider will have to provide the required services/equipment, if selected and declared as lowest evaluated bidder. In case selected bidder is not willing to supply/provide services on quoted amount then bid bond/security submitted with the bid will be forfeited in favor of the Commission.

30. Bidder must have regular **place of business, telephone numbers and email address and must provide proof of their existence in the particular business**. A brief profile of the bidder, along with list of major customers (corporate sector) along with their contact details (email/ mobile number) is required.

31. Items included in Compulsory Certification Scheme of PSQCA shall be duly certified by an accredited laboratory and fulfill necessary conditions of PSQCA, if applicable.

32. Bidder must submit following on **stamp paper of Rs.100, failing which the bid shall be rejected:**

    a) Affidavit that the documents/details/information submitted is true and liable to be rejected if proven false and in that case legal action is liable on that bidder.

    b) Affidavit that the bidder has never been blacklisted by any National/International organizations.

33. Comprehensive warranty & onsite support for mentioned years shall be given for the equipment/software/renewal at Islamabad, Karachi, and Lahore offices (if applicable). The solution however, will be deployed in HO, agent will be deployed remotely.

34. All software-based items contain installation and configuration and end user orientation which is responsibility of the supplier (if support is not provided by the Principal).

35. The equipment/software/renewals supplied must be duty paid in respect of all applied duties and taxes.

36. The quantities may increase/decrease according to SECP requirement.

37. The end user License, source codes, end user warranties and end user support services will be in the name of SECP for all equipment and software loaded on the equipment delivered.

38. A copy of valid authorized agency/partnership/dealership/distributorship certificate from their principals is to be submitted with the bid. (if applicable)

39. All payments shall be made after deduction of taxes and all payments shall be made through cross cheque in Pak Rupees. Taxes will be deducted at source as per Government Rules at the time of payment.

40. The bidders do not have the option of submitting their bids electronically. Telegraphic and conditional bids will not be accepted.

41. Only sealed bids will be accepted/opened and unsealed bids will be rejected.

42. Sealed bids may be dropped in the tender drop box placed at Ground Floor of the NIC Building, 63 Jinnah Avenue, Islamabad.

43. The bid bond/security of successful bidder will be retained and returned after delivery, installation and commissioning of complete equipment/licenses/services/renewals of ordered items/services. However, bid bond/security of unsuccessful bidders will be returned after award of contract to successful bidder.

44. During the retention period the bid bond/security no interest / markup will be provided on this amount by Commission to bidder at the time of refund/release of bid bond/security.

45. Successful bidders shall be bound to provide the required items/services within the delivery period. In case of late delivery, late delivery (LD) charges equivalent to 1% (of the PO/contract Value) per week shall be imposed and deducted from the payment. However, imposed penalty shall not exceed 10% of the PO/contract value.

46. In case 1st lowest bidder is unable to supply ordered items/services then the Commission reserve the right to award the contract to 2nd lowest evaluated bidder. In case 2nd lowest evaluated bidder is unable to supply ordered items/services then the Commission reserve the right to award the contract to 3rd lowest evaluated bidder.

47. Bid bond/security of the bidder who is unable to supply ordered items/services shall be forfeited in favor of the Commission.

48. The Commission reserves the right either to issue a Purchase Order or sign an agreement with the successful bidder OR PO & Agreement both will be executed.

49. The bids received after the due date and time will not be entertained.

50. It is of utmost importance that bids should be submitted very carefully and the instructions set forth above, scrupulously complied with, failing which the offer will be ignored.

51. Bids received will be evaluated as per evaluation criteria given in the TORs.

52. The place of bid destination is:

Securities and Exchange Commission of Pakistan,
NICL Building, 63 Jinnah Avenue, Blue Area, Islamabad.

53. The envelopes shall bear the following additional identification marks:

Bid for:	**Supply, Installaion and Configuration of Data Loss Prevention (DLP) and Enterprise Mobility Management (EMM) solution.**
Bidder Name:	XYZ
Attention:	M. Ubaidullah Khalid, Deputy Director (Admin) 4th Floor, NICL Building, 63 Jinnah Avenue Blue Area, Islamabad

54. The deadline for the submission of bids is:

Date: February 03, 2020
Time:1030Hrs

55. The bid opening shall take place at
Securities and Exchange Commission of Pakistan
NICL Building, 63 Jinnah Avenue, Blue Area, Islamabad
Date: February 03, 2020
Time: 1100Hrs

56. A statement "Not to be opened before 1100 Hrs on February 03, 2020" shall be clearly mentioned on the top of the sealed bid.

Note: Attachment Details are as under:

- Scope of Work, Functional Requirements and Technical Evaluation Criteria for DLP Solution **Annex "A"**
- Scope of Work, Functional Requirements and Technical Evaluation Criteria for Enterprise Mobility Management (EMM) solution. **Annex "B"**
- Common Requirements for Both (Annex – A and Annex- B) **Annex "C"**
- Documentary Evidence **Annex "D"**
- Financial Bid Submission Form **Annex "E"**
- Non- Disclosure Agreement **Annex "F"**
- Sample Agreement **Annex "G"**
- Clarifications of Pre-bid meeting dated January 09, 2020 **Annex "E"**

If the above terms and conditions are acceptable then bids must be submitted well in time and according to the requirements.

Annex – "A"

Scope of Work (SoW) /Functional Requirements (FRs) for DLP solution

1. Scope of Work (SoW):

Following is the scope of work:

1. Supply, installation, configuration of Data Loss Prevention (DLP) solution, covering:
    A. Data at Motion;
    B. Data at Rest; and
    C. Data in Use.
2. The bidder shall be responsible to configure and implement default and customized policies, policy fine tuning and monitoring as per SECP requirements.
3. Expected number of users of DLP solution will be approximately 700
4. The bidder /Principal shall provide maintenance and support for one (01) Year.
5. The bidder shall prepare and provide following documents: Guides /Manuals (will be part of the contract):
    A. Administration;
    B. Policy Management and Fine Tuning;
    C. Data Classification; and
    D. Incident management.
6. The bidder shall provide /arrange professional instructor-led, hands on training of the proposed solution for Administrators, End Users.

2. Functional Requirements and Evaluation Criteria:

1. Data Definition & Classification		
1.1	**By Content Type**: The solution should be able to classify data on the basis of content, such as: 1. Content with specific document properties; 2. File types; 3. Content with tags; 4. Encrypted content; and 5. Content categories.	Must
1.2	**By File Destination**: The solution should be able to classify data on the basis of where the content is being sent (i.e. out of organization).	Must
2. Risk Vector Coverage		
2.1	**Email /Webmail**: The solution should be able to monitor sensitive data sent through Emails and webmail.	Must

2.2	**PCs /Virtual Machines /Smartphones**: The solution should be able to monitor sensitive data stored or in use on: PCs; Virtual Machines; Laptops; running Windows 7, Windows 10, Windows server 2008, 2012, RedHat Linux	Must
2.3	**Social Media**: The solution should be able to monitor sensitive data sent through social media platforms.	Must
3. Data in Use Protection		
3.1	**Privileged User Monitoring**: The solution should be able to monitor the actions of privileged users with the ability to override DLP controls, perform mass data extracts, etc.	Must
3.2	**Access /Usage Monitoring**: The solution should be able to monitor access and usage of high-risk data to identify potentially inappropriate usage.	Must
4. Data in Motion Protection		
4.1	**Network Monitoring**: The solution should be able to log and monitor network traffic to identify and investigate inappropriate sensitive data transfer.	Must
4.2	**Internet Access Control**: The solution should be able to prevent users from uploading data through the web, through personal webmail, social media, online backup tools etc.	Must
5. Data-At-Rest		
5.1	**Network /Intranet Storage**: The solution should govern access to network-based repositories containing sensitive data on a least privilege basis.	Must
5.2	**Physical Media Control**: The solution should prevent the copying of sensitive data to unapproved media and ensure that authorized data extraction only takes place on encrypted media.	Must
6. Compliance Requirements		
6.1	**Compliance Management**: The solution must provide an incident tracking system that logs and monitors policy violations.	Must
6.1	**Compliance Monitoring:** The solution should provide an incident tracking system that logs and monitors policy violations.	Must
6.2	**Policy Violation Notifications**: The solution should be able to provide notifications for the policy violations occurring at the network or the endpoint.	Must

6.3	**Audit trail**: The solution should be able to maintain an audit trail of incidents.	Must
7. Whitelisting		
7.1	**Whitelist Files and Repositories**: The solution should allow users to define a list of files and repositories that are trusted and clean files so users do not have to remediate files that are safe for distribution.	Must
7.2	**Whitelist Devices**: The solution should be able to authorize the usage of a specific device for transfer of sensitive data.	Must
8. Application Management		
8.1	**Capability to enable application specific policies**: The solution should have the capability to enable application specific policies.	10
8.2	**Logs:** Successful and Failed attempts. Administrator Actions. Similarly, the solution /application should ensure that all attempts to execute an Administrative Command and changes in access to solution /application are logged (e.g. adding, modifying or revoking access). All logs are protected against tampering.	Must
9. Security Management		
9.1	**Integration:** The solution may support integration with data classification tools.	10
9.2	**Implementation and enforcement**: The solution should provide implementation and enforcement of corporate DLP security policies.	Must
9.3	**Enterprise Digital Rights Management:** The solutions may Support integration with EDRM.	10
10. Reporting		
10.1	**Reporting, dashboards and auditing capabilities:** The solution must have a mix of customizable and pre-built reports.	Must
10.2	**Incident Management**: The solution should have single /multiple incident management capability.	Must
10.3	**Centralized system status and administration interface:** The solution must have centralized standard system status and administration interface.	Must
10.4	**Hierarchical Endpoint Administration:** The solution must have option to show status and administration for endpoints.	10
10.5	**Policy Creation and Management:** The solution must have policy creation and management feature.	Must
11. Administration, Monitoring and Reporting [Management Console /Interface]		
11.1	**Default and custom policies /templates:** The solution must provide for built-in /predefined policies /templates.	Must
11.2	**Central /Single console /dashboard with Incident Repository:** The solution should provide centralized management console.	Must

11.3	**Role-based access**: The solution should provide role-based access for multiple administrators.	Must
11.4	**Monitoring the sensitive content with Visibility & Controls:** Solution must provide the ability to monitor the sensitive content being transferred.	Must
11.5	**Auditing of Administrators /Users of the Solution:** Solution must provide and maintain the audit logs /trails for the actions performed by the Administrators /Users of the Solution while accessing the solution so as to maintain an audit trail.	Must
11.6	**Monitor and prevent data leakage on endpoints:** Solution should provide an agent-based monitoring and prevention mechanism for endpoints.	Must
11.7	**Policies application basis:** Solution should provide the ability to apply policies based on the users /devices and groups.	Must
12. Lifecycle & Support		
12.1	The End of Life, End of Support life cycle of the proposed solution should be minimum 5 years.	Must
12.2	The Bidder /Principal must configure and implement default and customized policies, policy fine tuning and monitoring as per SECP requirements.	Must
12.3	The Bidder /Principal Support for 01 Year included in the proposed solution.	Must
12.4	The Bidder /Principal must provide /arrange professional instructor-led, hands on training of the proposed solution for Administrators, End Users.	Must

3. Final Requirements and Evaluation Criteria:

1	Total Marks in addition to MUST requirements	40
2	Minimum Marks in addition to MUST requirements	50%

Technical bid found in compliance to all the MUST requirements and securing 50% marks shall only be considered qualified for financial bid opening and at par/equivalent. Bid found lowest in financial bid opening shall be selected.

Annex – "B"

Scope of Work (SoW) /Functional Requirements (FRs) for MDM solution

1. Scope of Work (SoW):

Following is the scope of work:

1. Supply, installation and configuration of Enterprise Mobility Management (EMM) solution, covering:
    A. Mobile Application Management (MAM);
    B. Mobile Content Management (MCM); and
    C. Mobile Device Management (MDM).
2. The bidder shall be responsible to configure and implement default and customized policies, policy fine tuning and monitoring as per SECP requirements.
3. The bidder /Principal should provide maintenance and support for one (01) Year.
4. The bidder shall prepare and provide following documents: Guides /Manuals (will be part of the contract):
    A. Administration;
    B. Policy Management and Fine Tuning;
    C. Incident management; and
    D. Monitoring and Reporting.
5. The bidder shall provide /arrange professional instructor-led, hands on training of the proposed solution for Administrators, End Users.
6. Following pricing models are required for EMM (MDM)

Pricing options are separately required for:

1.100 Users
2.100 Devices
3.200 Users
4.200 Devices
5.300 Users
6.300 Devices
7.Per User
8.Per Device

2. Functional Requirements and Evaluation Criteria:

1. Device Management		
1.1	**Registration of device:** The solution must provide mobile device registration.	Must
1.2	**Selective wipe:**	Must

	The solution must provide selective (Corporate information removal) and full remote wipe.	
1.3	**Disabling hardware features:** The solution must provide the capability to disable hardware features. Disabling of required ports, protocols and services including disabling of camera, disabling of removable media card etc.	Must
1.4	**Configure the device features:** The solution must provide the capability to configure the device features. These include configuring Wi-Fi, configuring VPN, configuring proxy /gateway settings, and disabling access to public app store and restricting unverified applications etc.	Must
1.5	**Support multiple users per device:** The solution must support multiple users per device (auto-configure device settings based on who is logged on).	Must
1.6	**View the real-time mobile devices inventory list:** The solution must allow designated system administrators to view the real-time mobile devices inventory list and locate the devices.	Must
1.7	**Lock, unlock and reset password:** The solution must provide the ability to lock, unlock and reset password.	Must
2. Application Management		
2.1	**Capability to push mandatory apps:** The solution must provide the capability to push mandatory apps to the device during the registration process.	Must
2.2	**Segregating corporate information from PI:** The solution must be able to segregate corporate information from personal information (PI), and secure company information on the device preferably by using a secure container (or dual-persona) solution.	Must
2.3	**Capability to block copy /paste of information between apps and from email client:** The solution must able to provide the capability to block copy /paste of information between apps.	Must
2.4	**Capability to enable application specific policies:** The solution should have the capability to enable application specific policies.	10
2.5	**Lock down Kiosk mode:** The solution preferably provides for lock down Kiosk mode where user can only access specific apps and settings configured by the administrator.	10
2.6	**Logs:** Successful and Failed attempts of policy violations.	10
2.7	**Information dissemination capability:** The solution should be able to push announcements and provide user acceptance of terms and conditions.	10
2.8	**Implementation and enforcement:** The solution should be able to implement and enforce mobile device security policies.	Must
2.9	**Detecting and restricting compromised device:** The solution must be able to detect and restrict compromised devices, for example, iOS jail-broken devices and rooted Android devices.	Must
2.10	**Filter (restrict) noncompliant devices:** The solution must be able to filter (restrict) non-compliant devices from accessing the corporate servers (e.g., email) as well as trigger notifications.	Must
2.11	**Device-level encryption:**	10

	The solution should be able to provide device-level encryption capability.	
2.12	**Encrypted data:** The solution should ensure that data transmitted over a network connection, stored on Electronic Media /removable Media /on a mobile computing device /Media is encrypted.	Must
2.13	**Remote Administration over an encrypted network connection:** The solution ensures that Remote Administration of System is performed over an encrypted network connection.	Must
2.14	**Disabling Auto-run for removable electronic storage media:** The solution can disable auto-run for removable electronic storage media (e.g. CDs, DVDs, USB drives, etc.) and network drives.	Must
3. Miscellaneous		
3.1	**Compliance:** The solution may be compliant with PII, PCI, SOX, HIPAA, FERC, GLBA & others standards.	10
4. Specification –General Requirements		
4.1	**Unified Endpoint Management (UEM):** The solution should be able to a single management interface for mobile, PC and other devices.	10
4.2	**OS Supports:** Supporting all the mainstream mobile and desktop OS (Android, IOS and Windows).	Must
4.3	**Single sign on component:** The solution must be able to provide single sign on component that support SAML 2.0 authentication for web application and also single sign-on for mobile applications.	10
4.4	**Conditional access for users:** The solution should be able to provide conditional access for users to access corporate content and applications.	10
4.5	**Whitelisted apps:** The solution should allow the administrators to provide whitelisted apps to be shared with end users.	Must
5. Self-Service portal for users		
5.1	**User registers and de-registers with devices:** The solution must provide the capability to allow user to register and de-register devices on their own through online self-service portal.	Must
5.2	**Limiting the number of devices, a user can register:** The solution must allow the configuration to limit the number of devices a user can register using self-service portal, as well as specific device types and OS versions that can be registered.	Must
5.3	**Integrating with Customer LDAP (Active Directory):** The solution must be able to integrate with Customer LDAP (Active Directory) to authenticate staff when accessing the self-service portal.	Must
5.4	**Self-Service portal supports:** The Self-Service portal must be browser independent or at least support all common internet browser.	Must
5.5	**Reporting, dashboards and auditing capabilities:** The solution must have a mix of default and customizable reports and tools.	Must
5.6	**Incident Reporting on Central Dashboard:**	Must

	The solution must provide a central dashboard/ screen for incident handlers to monitor and manage policy violations.	
5.7	**Standard system status and administration interface:** The solution must have standard system status and administration interface, including user and group administration.	Must
6. Administration, Monitoring and Reporting [Management Console /Interface]		
6.1	**Managing deployments and the mobile devices:** The solution must provide the capability to the administrators to manage the deployments as well as manage the mobile devices.	Must
6.2	**Default and custom policies /templates:** The solution must support default and custom policies. Default policies are applied to all devices. Custom policies are applied to selective devices, and may replace the default policies.	Must
6.3	**Role-based access:** The solution must provide role-based access for normal users and administrators.	Must
6.4	**Auditing of Administrators /Users of the Solution:** The solution must provide and maintain the audit logs /trails for the actions performed by the Administrators /Users of the solution while accessing the solution so as to maintain an audit trail.	Must
7. Lifecycle & Support		
7.1	The End of Life, End of Support life cycle of the proposed solution should be minimum 5 years.	Must
7.2	The Bidder /Principal must configure and implement default and customized policies, policy fine tuning and monitoring as per SECP requirements.	Must
7.3	The Bidder / Principal support for 01 Year included in the proposed solution.	Must
7.4	The Bidder /Principal must provide/ arrange professional instructor led, hands on training of the proposed solution for Administrators, End Users.	Must

3. Final Requirements and Evaluation Criteria:

1	Total Marks in addition to MUST requirements	90
2	Minimum Marks in addition to MUST requirements	50%

Technical bid found in compliance to all the MUST requirements and securing 50% marks shall only be considered qualified for financial bid opening and at par/equivalent. The Commission reserves the right to select any option as per its requirement i.e. Annex B, Clause 6. Bid found lowest in price to that specific option in its financial bid opening shall be selected.

Annexure – "C"

Common Requirements for Both Annexure – A and Annexure - B

1. General Requirements and Evaluation Criteria

S. No.	Description	Marks
1.	Complete compliance with SOW, Functional requirements, Training requirement, Project Activities and Project Management	**MUST**
2.	The service provider should have delivered and deployed similar solutions in public or private sector. Work order from at least 01 client should be attached as proof with contact details of reference. The feedback may be obtained from the reference provided.	**MUST**
3.	The service provider should have at least one (01) certified resource of the with minimum of 02 years' experience of the offered product. Attach copy of all relevant certificates as proof.	**MUST**
4.	The bidders **MUST** submit a technical compliance sheet (Section 5) against all requirements mentioned in the Functional and General evaluation criteria	**MUST**
5.	Professional hands on and instructor led training for at least four (4) resources of the offered solution(s)	**MUST**
6.	Gartner Magic Quadrant 2018 /2019 rating of offered solution (Challengers & Leaders only), attach proof	**MUST**
7.	Principal Authorization Letter for Tender Participation	**MUST**
8.	Valid Partnership Letter with Principal/ Manufacturer	**MUST**

NOTE:

Bids NOT in compliance with any MUST item/requirement in the evaluation criteria, will NOT be evaluated.

2. Training Details:

Selected bidder shall provide the training to the SECP's personnel as described below:

A. The training should include the architecture, hardware, software, integration, and customization, policy installation, troubleshooting reporting and other aspects of the solutions.

B. The Bidder shall train SECP personnel for independent operation, creation of policies /rules, generation of reports, and analysis of the reports, troubleshooting and familiarization of features and functionalities, policy configuration, alert monitoring etc. post implementation

C. Bidder should submit detailed course content and provisional agenda along with the bid.

3. Project Activities (will be made part of the Contract)

Participating vendors are required to submit their proposals specifically covering the following activities and functions to be assessed (with full scope, unless otherwise restricted).

1.	Deployment of solutions in SECP HO Data Centre & SECP Data Recovery Center	Installation & Configuration and migration of existing Controls, Policies & Access rules
2.	LDAP Integration	Integration with active directory multi domains environment for user's authentication
3.	Reporting & Dashboards	Configuration of real time performance dashboard Daily, Weekly & Monthly reports
4.	Monitoring of Services	Integration with Monitoring Tool and integration with current SIEM solution
5.	DR Readiness	Configuration and testing with DR perspective
6.	Documentation	Design Documents, SOPs, User /Configuration /Admin Manuals
7.	Trainings	Trainings for at least 04 participants as mentioned in training details

4. Project Management

The selected vendor is expected to deploy DLP and Enterprise Mobility Management (EMM) solutions in SECP environment and deliver the following documentation in specified format as part of the scope of work (SoW).

1.	Start of the Project	a)	Presentation from the vendor at SECP HO, explaining the comprehensive project plan that includes tasks, procedures, tools, timelines, impacts, responsible persons, and report formats (Microsoft PowerPoint)
2.	Middle of the Project	a)	Weekly progress report on all tasks (Microsoft Excel /Project)
3.	End of the Project	a)	A detailed report covering the overall progress of the project
		b)	A consolidated product deployment report covering the whole commitment, including different tests results and recommendations about best practices
		c)	An executive-level presentation from the vendor at SECP HO explaining the project results and final reports (Microsoft PowerPoint)

5. Format for Compliance Sheet:

S. No.	Requirement	COMPLIANCE (YES/NO/ PARTIAL)	COMPLIANCE PROOF (PAGE NUMBER IN BID)

Annexure – "D"

DOCUMENTARY EVIDENCE

Name of the Bidder: _____

Bid against Reference No: _____

Date of opening of Bid: _____

Documentary evidence for determining eligibility of the bidders & evaluation of bids. Bidders should only initial against those requirements that they are attaching with the form. Bidders are required to mention the exact page number of relevant documents placed in the Bid. Bidders are advised to attach all supporting documents with this form in the order of the requirement.

S#	Required Documentation	Signature of Bidder	Supporting Document's Name	Page Number in the Bid.
1	NTN Certificate			
2	GST Certificate			
3	Availability on Active Tax Payers List of FBR			
4	Registration/Incorporation/Business Certificate			
5	Affidavits			
6	Bid Bond/Security (As applicable)			
7	Bid Validity period of 150 days (As applicable)			
8	Original Bidding documents duly signed/ stamped			

Annexure – "E"

FINANCIAL BID SUBMISSION FORM

The bidder shall complete the matrix below by providing prices for the quoted solution(s) to be provided under this invitation. The resulting contract shall be a fixed price.

A. Supply, Installation and Configuration of Data Loss Prevention (DLP) solution

Deliverables	Total Quoted Price (Rs.)* Incl. of all applicable taxes
Supply, Installation and Configuration of Data Loss Prevention (DLP) solution	

B. Supply, Installation and Configuration of Enterprise Mobility Management (EMM) solution

Deliverables	Total Quoted Price (Rs.)* Incl. of all applicable taxes
Supply, Installation and Configuration of Enterprise Mobility Management (EMM) solution	

Bidder shall share breakup of the total quoted price of the quoted functionality/solution.

Note:

- Bidder may submit its bid against any one of the required functionality/solution.
- In case a bidder offers/quotes a solution comprising of both functionalities/solutions then
    - The bidder MUST quote separate price against each functionality/solution.
    - The bidder shall be able to supply, install and configure only one functionality/solution out of both, if declared as lowest evaluated bidder, against that functionality/solution.

Annex "F"

Sample Non-Disclosure Agreement (NDA)

This agreement is made the on _____ between:

(1) The Information Systems and Technology Department (IS&TD), Securities and Exchange Commission of Pakistan (the "SECP"), NIC Building, Jinnah Avenue, Blue Area, Islamabad

and

(2) Bidder Name, Office Address _____

hereinafter referred to as "Parties" collectively and the party disclosing shall be referred as "Disclosing Party" and the party receiving information shall be referred as "Receiving Party". For the purpose of preventing the unauthorized disclosure of Information as defined below, these parties agree to enter into a confidential relationship with respect to the disclosure of certain proprietary and information ("Information").

Background:

The Parties wish to discuss investment and collaboration opportunities relating to SECP's Information Systems and Technology Department business models and/or the technical and commercial capabilities of various technologies and projects ("Opportunities and Technologies") developed by one or more of the Parties. The Parties wish to mutually disclose certain Security Classified Information (SCI) to enable each of them to fully assess the Opportunities and Technologies.

It is agreed that:

In consideration for the mutual disclosures, the Parties agree to the terms of this Non-Disclosure Agreement (NDA):

1. "Information" means all information, data, ideas, innovations or material disclosed by any of the Parties relating to the Opportunities and Technologies, whether or not marked or designated as confidential, including, but not limited IS&TD's information to business plans, business proposals, projects, financial information, customer/company lists, prospective customers, technical proposals, product descriptions, hardware specifications, software in both source and object code, computer outputs, computer interfaces, application program interfaces, computer calls, flow charts, data, drawings and know-how.

Each Party's Obligations:

2. Each Party will:
    a. Keep the Information disclosed to it by any disclosing Party confidential and secure, and in addition apply the same degree of care and the same controls which that Party applies to his or its own trade secrets.
    b. Use or make copies of the Information disclosed to it solely to assess the Opportunities and Technologies. Any such copies shall remain the property of the disclosing Party and be distributed or otherwise be made available internally within the receiving Parties on a need to know basis.
    c. Give immediate notice to the disclosing Party if a receiving Party knows of or suspects that there has been any unauthorized use or disclosure of Information arising through a failure by a Party to keep the Information confidential.

Publicity:

3. No receiving Party will without the prior consent in writing of the disclosing Party either release any press statement or issue any other publicity regarding the existence, scope, objective, conduct, performance or results of any proposed or actual contract between any of the Parties.

Exclusions:

4. The provisions of this Agreement shall not apply to Information:
    a. which a receiving Party can prove to the reasonable satisfaction of the disclosing Party was lawfully in his or its possession at the time of disclosure and was not acquired either directly or indirectly from the disclosing Party; or
    b. which is lawfully generally known (other than due to the negligent act or omission of Parties or his breach of this Agreement); or
    c. which the receiving Party obtains from a third party which was entitled to disclose that Information to the receiving Party without any restriction.

Various Obligations:

5. Each receiving Party agree that he or it shall not acquire any right in or title to or license in respect of the Information disclosed to it or any intellectual property rights embodied in the Information. The rights provided to the Parties under this Agreement are personal to the Parties and shall not be assigned or transferred to any other party whatsoever.
6. The obligations under this Agreement shall continue as regards any item of Information until it is lawfully generally known or is otherwise not subject to the provisions of this Agreement. Since the information available with SECP is highly confidential, the receiving party shall never be allowed to disclose such information so the receiving party shall not be allowed to disclose the information even after the expiry of the agreement.
7. On the written request of a disclosing Party at any time, each receiving Party agrees to:
    a. promptly return or procure the return of or destroy (at the disclosing Party's option) all or some (as the disclosing Party may direct) of the originals and copies of the Information under his or its care or control and
    b. confirm in writing that this has been done and that no Information or copies exist under the receiving Party's care or control and
    c. Not use the Information for any other purpose whatsoever.
8. Nothing in this Agreement prevents disclosure of the Information to any persons or bodies having a legal right or duty to have access to or knowledge of the Information.
9. This Agreement constitutes the entire agreement and understanding between the parties with respect to its subject matter and replaces all previous NDA agreements between, or undertakings by the parties with regard to such subject matter. This Agreement cannot be changed except by written agreement between the parties.
10. (i) All disputes arising out of all disputes arising out of or in connection with the present agreement shall be settled through Arbitration. Each Party shall appoint an arbitrator and the appointed arbitrators shall commence the proceedings. In case of difference of opinion between an even number of appointed arbitrators, the matter shall be referred to an umpire mutually appointed by the arbitrators. The umpire shall then make an award which shall be final and binding. Prior to initiation of arbitration proceedings, the aggrieved Party shall give the other Party written notice describing the claim and amount as to which it intends to initiate action.

    (ii) The place of arbitration shall be Islamabad, the arbitration shall be governed by the Arbitration Act, 1940 and the language of the arbitration shall be English.

Signed for and on behalf of
Information Systems and Technology Department, Securities and Exchange Commission of Pakistan

Name:
Designation:

_____

Signed for and on behalf of

Bidders

Name:
Designation:

_____

Witness No. 1:
Name:
Address:
NIC:

_____

Witness No. 2:
Name:
Address:
NIC:

_____

Annexure – "G"

SAMPLE AGREEMENT

This agreement ("Agreement") is made on this_____ day of _____ 2020,

By and Between

Securities & Exchange Commission of Pakistan, a statutory body established in pursuance of the Securities and Exchange Commission of Pakistan Act, 1997 ("SECP Act 1997"), having its Head Office at NICL Building, 63-E, Jinnah Avenue, Islamabad, Pakistan (hereinafter referred to as the **"Commission"** which expression shall be deemed to include, where the context so permits, its successors in interests, administrators and permitted assigns) OF THE ONE PART;

And

XYZ (Pvt.) Limited having its registered **Office Address**, Pakistan (herein after referred to as the **"Contractor"** which expression shall be deemed to include, where the context so permits, its successors in interests, administrators and permitted assigns) OF THE OTHER PART;

The Commission and the Contractor may hereinafter individually be referred to as Party and collectively as Parties.

WHEREAS:

A- The Commission requires DLP/EMM solution from a competent Firm/Company dealing in DLP/EMM Solution and Services for published requirement at its Head Office Islamabad and branch Offices.

B- The Contractor represents and warrants that it has the requisite expertise and resources to provide the services required by the Commission.

C- The Contractor has agreed and the Commission has approved the Services to be provided by the Contractor on the terms and conditions mentioned herein Annex – A/B.

Now, therefore, in consideration of the mutual covenants and agreements herein contained, the parties hereto, intending to be legally bound, agree as follows:

1-Duration

1-1. This Agreement will become effective as of _____ and will remain in effect for a period of _____ (the "Term"). The termination of this Agreement will not:

(a) relieve either party from any expense, liability or obligation or any remedy therefore which has accrued or attached prior to the date of such termination, nor.

(b) cause either party to lose, surrender or forfeit any rights or benefits which have accrued at the time of termination.

1-2. Prior to the expiration of the term, this Agreement may be extended for a further period by mutual agreement between the parties, provided that, the parties must enter in to a mutual written agreement to extend the term. When used in this agreement, the phrase "the Term" shall refer to the entire duration of the Agreement.

2-Scope of Work

2-1. The Services to be provided by the contractor under this Agreement shall be in accordance with Annex-A/B.

3- Payments

3-1. The Contractor will charge the Commission a fixed amount of PKR XXX (inclusive of all taxes) for. The payment will be made as per payments terms mentioned herein after.
1. After Delivery of Licenses /Software60%
2. After Installation and Configuration20%
3. After Professional Training20%

3-4. The Commission will ensure timely payments within forty-five (45) days of the receipt of an invoice from the Contractor.

3-5. Any payments made under this Agreement by the Commission shall be less any Government taxes, which the Commission is authorized under the law to deduct.

4-Contractor Obligations

4-1. The Contractor will engage its own qualified employees / staff at the premises.

4-2. The Contractor will be exclusively responsible for all legal benefits to its staff / employees including compensation for death, injury etc. while performing the Contractor's obligations under this Agreement and the Commission shall have no obligation or responsibility on any account whatsoever.

4-3. The Contractor shall be responsible for all acts or omissions of any of its staff or personnel working on the Commission's premises and shall be liable for any loss or damage suffered by the Commission and shall compensate the Commission accordingly.

4-4. The Contractor will indemnify the Commission against all the damages or losses etc. that may be caused by his staff / employees due to any reason whatsoever, including but not limited to theft, malignance and pilferage etc.

4-5. The work done and standards observed / maintained by the Contractor will be checked, inspected and reviewed by the authorized officer(s) of the Commission to ensure that the work is being done and standards are observed as per terms of the Agreement and agreed specification, who may issue or give such notice, advises or reminders to the Contractor as may be necessary for the proper execution of the Agreement.

4-6. The authorized officers of the Commission will at all the time have free access to all part of the work area where the work carried out by the Contractor is in progress. The Contractor will extend all possible help and facilitate as may be required by Commission.

4-7. The billing invoice of the Contractor will be verified by authorized officer(s) of the Commission to check whether the Contractor has fulfilled his obligations as per terms of the Agreement and the payment will be made to the contractor accordingly.

4-8. The Contractor shall ensure that it obtains the necessary insurance coverage for its staff employees deputed at the premises for any loss or damage.

5- Termination

5-1. This Agreement may be terminated by either party by providing thirty (30) days prior written notice to the other party if the other party is in material breach of its obligations under this Agreement and the breach has not been remedied for a period of fifteen (15) days after the notice has been issued.

6- Dispute Resolution

If any dispute arises at any time between the parties:

6-1. The parties shall endeavor to resolve such differences amicably.
6-2. In the event of that such differences cannot be resolved within a period of fifteen (15) days: the matter shall be referred to the Departmental Head IT of the Commission, whose decision shall be final and binding on both the parties.

7- Force Majeure

7-1. Any failure or omission by any party to perform any obligation under this Agreement shall not be deemed a breach to the extent that such failure or omission is caused by any supervening event (event of the force majeure) beyond the reasonable control of party so effected (to include but not limited to acts of God, acts of Government, war explosions, terrorism, sabotage, natural disaster, riots, civil commotion, strikes, labor disputes and break down of communication system etc.) and which by the exercise of reasonable diligence could not be prevented or provided against and effects of which by could not be overcome by reasonable expenditure.

7-2. The party so affected by an event of force majeure shall as soon as it becomes aware of the occurrence thereof, immediately notify the other party, the party so effected shall do all that is reasonably possible to remove or ameliorate the effect of such an event of force majeure. If all reasonable efforts fail or if the event of force majeure persists beyond a period of thirty (30) days, either party may terminate this Agreement with immediate effect.

8- Governing Law and Jurisdiction

8.1 This agreement shall be governed by and construed in accordance with the laws of the Islamic Republic of Pakistan.

8.2 Disputes arising out of this Agreement are subject to the exclusive jurisdiction of the courts of Islamabad, to which the Parties irrevocably submit.

9- Amendment

This Agreement and schedules thereto shall not be amended except by the mutual consent in writing of both the parties.

10- Assignment

The Contractor shall not assign this Agreement or any of its obligations hereunder, either in whole or any part, to any other person in any form or manner what so ever, without the prior written consent of the Commission.

11- Waiver

The failure of any party to exercise any right or the waiver by any party of any breach, shall not prevent a subsequent exercise of such a right or be deemed a waiver of any subsequent breach of the same or any other provision of this Agreement.

12- Entire Agreement

This Agreement along with the schedules constitutes the entire agreement between the parties in respect of the subject matter hereof and supersedes all prior oral or written arrangements.

13- Severance

If any one or more provisions of this Agreement shall for any reason be held to be invalid, illegal or unenforceable in any respects, such provision (s) shall be limited, modified or severed as necessary to eliminate the invalidity, illegality or unenforceability and all other provisions of this Agreement shall remain unaffected.

14- Notice

14-1. Any notice, request or consent made pursuant to this Agreement shall be in writing and shall be deemed to have been made when delivered in person to an authorized representative of the party to whom the communication is addressed, or when sent by registered mail, facsimile or electronic mail to such party at the contact details detailed below.

To the Commission:

Securities and Exchange Commission of Pakistan
NIC Building 63, Jinnah Avenue,
Islamabad

Telephone 051-9207092-4
Facsimile: 051-9204915
E-mail:

To the Contractor:
Mr. XYZ
Designation
XYZ (Pvt.) Ltd
Address

Telephone XXX-XXXXXXX
E-mail:

14-2. A party may change its contact details by providing notice thereof to the other party without having to amend this agreement in accordance with this article.

15- Confidentiality

15-1. The Contractor undertakes and shall ensure the complete confidentiality of all and any information in respect of this agreement and the services stated herein, including without limitation the communication to and by the Commission about any of its business information. The Contractor shall not disclose any such information to any person.

15-2. The Contractor shall keep strictly confidential any and all business and technical information that may be disclosed or confided to it by the Commission or which the Contractor or any of its employees / staff may obtain directly or indirectly during the course of performance of this Agreement.

15-3. It shall keep strictly confidential any and all information that may divulge upon it or any of its personnel during the course of performance of this agreement. It shall not disclose any such information to any person or allow utilization of the same in any person. The terms of confidentiality as applicable on the employees of the Commission in terms of SECP Act 1997 shall be applicable on all the staff and personnel of Contractor working in the premises.

15-4. In order to ensure confidentiality, Non-Disclosure Agreement i.e. **Schedule-B,** shall be signed by both the parties.

16- Integrity Pact

DECLARATION OF FEES, COMMISSION AND BROKERAGE ETC. PAYABLE BY THE SUPPLIERS OF GOODS, SERVICES & WORKS IN CONTRACTS WORTH RS.10.00 MILLION OR MORE

(Successful Bidder) hereby declares that it has not obtained or induced the procurement of any contract, right, interest, privilege or other obligation or benefit from Government of Pakistan or any administrative subdivision or agency thereof or any other entity owned or controlled by it (GoP) through any corrupt business practice.
Without limiting the generality of the foregoing (Successful Bidder) represents and warrants that it has fully declared the brokerage, commission, fee etc. paid or payable to anyone and not given or agreed to give and shall not give or agree to give to anyone

within or outside Pakistan either directly or indirectly through any natural or juridical person, including its affiliate, agent, associate, broker, consultant, director, promoter, shareholder, sponsor or subsidiary, any commission, gratification, bribe, finder's fee or kickback, whether described as consultations fee or otherwise, with the object of obtaining or inducing the procurement of a contract, right, interest, privilege or other obligation or benefit in whatsoever form from GoP, except that which has been expressly declared pursuant hereto.

(Successful Bidder) certifies that it has made and will make full disclosure of all agreements and arrangements with all persons in respect of or related to the transaction with GoP and has not taken any action or will not take any action to circumvent the above declaration, representative or warranty.

(Successful Bidder) accepts full responsibility and strict liability for making and false declaration, not making full disclosure, misrepresenting fact or taking any action likely to defeat the purpose of this declaration, representation and warranty. It agrees that any contract, right interest, privilege or other obligation or benefit obtained or procured as aforesaid shall, without prejudice to any other right and remedies available to GoP under any law, contract or other instrument, be voidable at the option of GoP.

Notwithstanding any rights and remedies exercised by GoP in this regard, (Successful Bidder) agrees to indemnify GoP for any loss or damage incurred by it on account of its corrupt business practices and further pay compensation to GoP in an amount equivalent to ten time the sum of any commission, gratification, bribe, finder's fee or kickback given by (Successful Bidder) as aforesaid for the purpose of obtaining or inducing the procurement of any contract, right, interest, privilege or other obligation or benefit in whatsoever form from GoP.

17- Relationship

The parties hereby agree that no terms of this Agreement shall be construed as to portray and employer-employee relationship between the parties and that both the parties are acting independently and at their entire discretion.

18- Stamp Duty

This Agreement shall be stamped in accordance with Stamp Act, 1899 by the Contractor.

19- Schedules & Annexure

Any and all schedules and annexures to this Agreement shall be deemed to be an integral part of this Agreement and shall be construed accordingly.

In witness hereof the parties hereto have executed this agreement on the date and at the place first above mentioned.

For Securities and Exchange Commission of Pakistan

For XYZ

Name: _____

Name: _____

Title _____ Title: _____

Witness Witness

_____ _____

(Terms and Conditions may change at the time of signing off by both parties with mutual agreement)

Scope of Work (SoW) /Functional Requirements (FRs) for DLP solution

1. Scope of Work (SoW):

Following is the scope of work:

1. Supply, installation, configuration of Data Loss Prevention (DLP) solution, covering:
    D. Data at Motion;
    E. Data at Rest; and
    F. Data in Use.
2. Configure and implement default and customized policies, policy fine tuning and monitoring as per SECP requirements.
3. Prepare and provide following documents: Guides /Manuals
    A. Administration;
    B. Policy Management and Fine Tuning;
    C. Data Classification; and
    D. Incident management.
4. Instructor-led, hands on training of the proposed solution for 04 Administrators.
5. Application usage training for End users in all SECP offices

2. Training Details:

Selected bidder shall provide the training to the SECP's personnel as described below:

A. The training should include the architecture, hardware, software, integration, and customization, policy installation, troubleshooting reporting and other aspects of the solutions.

B. The Bidder shall train SECP personnel for independent operation, creation of policies /rules, generation of reports, and analysis of the reports, troubleshooting and familiarization of features and functionalities, policy configuration, alert monitoring etc. post implementation

C. Bidder should submit detailed course content and provisional agenda along with the bid.

3. Project Activities

1.	Deployment of solutions in SECP HO Data Centre & SECP Data Recovery Center and all clients	Installation & Configuration and migration of existing Controls, Policies & Access rules
2.	LDAP Integration	Integration with active directory multi domains environment for user's authentication
3.	Reporting & Dashboards	Configuration of real time performance dashboard Daily, Weekly & Monthly reports
4.	Monitoring of Services	Integration with Monitoring Tool and integration with current SIEM solution
5.	DR Readiness	Configuration and testing with DR perspective
6.	Documentation	Design Documents, SOPs, User /Configuration /Admin Manuals
7.	Trainings	• Trainings for at least 04 participants as mentioned in training details • End user training

4. Project Management

1.	Start of the Project	a)	Presentation from the vendor at SECP HO, explaining the comprehensive project plan that includes tasks, procedures, tools, timelines, impacts, responsible persons, and report formats (Microsoft PowerPoint)
2.	Middle of the Project	a)	Weekly progress report on all tasks (Microsoft Excel /Project)
3.	End of the Project	a)	A detailed report covering the overall progress of the project
		b)	A consolidated product deployment report covering the whole commitment, including different tests results and recommendations about best practices
		c)	An executive-level presentation from the vendor at SECP HO explaining the project results and final reports (Microsoft PowerPoint)

Scope of Work (SoW) /Functional Requirements (FRs) for MDM solution

1. Scope of Work (SoW):

Following is the scope of work:

1. Supply, installation and configuration of Enterprise Mobility Management (EMM) solution, covering:
    - **A. Mobile Application Management (MAM);**
    - **B. Mobile Content Management (MCM); and**
    - **C. Mobile Device Management (MDM).**
2. Configure and implement default and customized policies, policy fine tuning and monitoring as per SECP requirements.
3. Prepare and provide following documents: Guides /Manuals
    - A. Administration;
    - B. Policy Management and Fine Tuning;
    - C. Incident management; and
    - D. Monitoring and Reporting.
4. Professional instructor-led, hands on training of the proposed solution for 04 Administrators.
5. Application usage training for End users in all SECP offices

2. Project Activities

1.	Deployment of solutions in SECP HO Data Centre & SECP Data Recovery Center and all clients	Installation & Configuration and migration of existing Controls, Policies & Access rules
2.	LDAP Integration	Integration with active directory multi domains environment for user's authentication
3.	Reporting & Dashboards	Configuration of real time performance dashboard Daily, Weekly & Monthly reports
4.	Monitoring of Services	Integration with Monitoring Tool and integration with current SIEM solution
5.	DR Readiness	Configuration and testing with DR perspective
6.	Documentation	Design Documents, SOPs, User /Configuration /Admin Manuals

7.	Trainings	• Trainings for at least 04 participants as mentioned in training details • End user training

3. Project Management

1.	Start of the Project	a)	Presentation from the vendor at SECP HO, explaining the comprehensive project plan that includes tasks, procedures, tools, timelines, impacts, responsible persons, and report formats (Microsoft PowerPoint)
2.	Middle of the Project	a)	Weekly progress report on all tasks (Microsoft Excel /Project)
3.	End of the Project	a)	A detailed report covering the overall progress of the project
		b)	A consolidated product deployment report covering the whole commitment, including different tests results and recommendations about best practices
		c)	An executive-level presentation from the vendor at SECP HO explaining the project results and final reports (Microsoft PowerPoint)

Annex "E"

Clarifications of Pre-bid meeting dated January 09, 2020 - Supply, Installation and Configuration of Data Loss Prevention (DLP) solution / Supply, Installation and Configuration of Enterprise Mobility Management (EMM) solution.

Q No.	Original Statement	Vendor Question	SECP Response
1	**By Content Type:** The solution should be able to classify data on the basis of content, such as: 1. Content with specific document properties; 2. File types; 3. Content with tags; 4. Encrypted content; and 5. Content categories	By "classify data", we are assuming that this term means that the DLP Solution should be able to "detect sensitive data" on the basis of content. (Kindly confirm if our understanding is correct so that we can Fully Comply with this requirement)	Yes, DLP solution should be able to detect/identify data based on content as mentioned.
2	**By File Destination:** The solution should be able to classify data on the basis of where the content is being sent (i.e. out of organization).	We are assuming that the expectation here is that the DLP Solution must be able to detect the sensitive content and where it is being sent via email (email addresses, domain) and based on the configured DLP Policy can apply different response actions depending on where it is being sent. (Kindly confirm if our understanding is correct so that we can Fully Comply with this requirement)	Yes, DLP should be able to identify classified data and apply various policies, based on that data can be send to authorized destinations.
3	**PCs /Virtual Machines /Smartphones:** The solution should be able to monitor sensitive data stored or in use on: 1. PCs; 2. Virtual Machines; 3. Laptops; and 4. Smartphones 5. Tablets etc.	The DLP Solution can indeed monitor the sensitive data stored or in use on supported operating systems (Windows, Mac) running on PC's, Virtual Machines and Laptops via the Endpoint Agent however for Smartphones and Tablets there is no Agent. We will have to Partially Comply with this requirement if Smartphones/Tablets are part of the DLP Solution and not the MDM Solution for this specific requirement. (Kindly confirm if the Smartphones/Tablets are part of the DLP Solution or the MDM Solution)	Smartphones and Tablets are removed from this list and will not be considered for final evaluation
4	**Social Media**: The solution should be able to monitor sensitive data sent through social media platforms.	On the Managed Endpoints, the sensitive data can be monitored which is sent via supported browsers to social media platforms. On the Network, if there is a supported web proxy deployed we can integrate with it to monitor the sensitive data sent that is passing through the Web proxy.(Kindly confirm if our understanding is correct and therefore we can Fully comply with this requirement)	Yes, If any employee tries to upload confidential document on social media platform, it will be blocked by DLP.
5	**Privileged User Monitoring:** The solution should be able to monitor the actions of privileged users with the ability to override DLP controls, perform mass data extracts, etc.	We assume that the expectation here is that the DLP Policy should be able to be configured in a monitor only mode for privileged users so that their actions are only monitored and not blocked.(Kindly confirm if our understanding is correct and therefore we can Fully comply with this requirement)	Administrative will always have full privileges due to centralized control solution, but his/her activities can be logged separately which will be controlled by Super Admin.
6	**Access /Usage Monitoring:** The solution should be able to monitor access and usage of high-risk data to identify potentially inappropriate usage.	We assume that the expectation here is that the DLP Solution should provide the list of incidents generated via the access/usage of sensitive high-risk data as identified by the configured DLP Policy thereby allowing the investigators to generate reports and identify potentially inappropriate usage.(Kindly confirm if our understanding is correct and therefore we can Fully comply with this requirement)	Yes
7	**Network Monitoring:** The solution should be able to log and monitor network traffic to identify and investigate inappropriate sensitive data transfer.	The DLP Solution can be integrated in passive mode with a network egress point such that it receives via SPAN/TAP network traffic (unencrypted) which it can analyze and apply the configured DLP Policies in passive mode. The investigator can view the incidents list to identify inappropriate sensitive data transfer. (Kindly confirm if our understanding is correct and therefore we can Fully comply with this requirement)	The solution should be able to log and monitor network traffic to identify and investigate inappropriate sensitive data transfer.
8	**Internet Access Control:** The solution should be able to prevent users from uploading data through the web, through personal webmail, social media, online backup tools etc.	We assume that the expectation here is that on the Managed Endpoints the DLP Solution should monitor the users uploading or sending data outside through monitored supported applications/browsers. On the Network, if there is a supported web proxy deployed we can integrate with it to monitor the sensitive data sent that is passing through the Web proxy.(Kindly confirm if our understanding is correct and therefore we can Fully comply with this requirement)	Yes
9	**Mobile Device Protection:** The solution should harden mobile device configurations and enable features such as password protection and remote wipe facilities and prevention of unencrypted transfer of documents.	This requirement seems to be for the MDM Solution.(Kindly confirm that this requirement is for the MDM Solution and not for the DLP Solution so we can ignore it in preparing the compliance sheet)	This condition has been removed and will not be considered for evaluation
10	**Endpoint Security:** The solution should restrict access to local admin functions such as the ability to install software and modify security settings.	This requirement does not seem to be for the DLP Solution rather it's something possibly catered for by an Endpoint Security Solution. (Kindly confirm that this requirement is not for the DLP Solution so we can ignore it in preparing the compliance sheet)	This condition has been removed and will not be considered for evaluation
11	**Network /Intranet Storage:** The solution should govern access to network-based repositories containing sensitive data on a least privilege basis.	This requirement does not seem to be for the DLP Solution. What the DLP Solution can do is identify the sensitive content stored on network-based repositories and apply response actions such as Quarantine etc.(Kindly confirm that this requirement is not for the DLP Solution or our explanation for what a DLP Solution can do is the actual requirement)	Unauthorized user cannot access any confidential data even it is placed on network repositories. The solution can do it by identifying contents stored on data and by applying configured DLP policies through Access Management.
12	**Physical Media Control:** The solution should prevent the copying of sensitive data to unapproved media and ensure that authorized data extraction only takes place on encrypted media.	We assume that the expectation here is that the DLP Solution should be able to recognize the authorized removable media by attributes such as Device ID. The sensitive data will be prevented from copying when the removable media is not authorized or allowed in the configured DLP Policy. (Kindly confirm if our understanding is correct and therefore we can Fully comply with this requirement)	The solution should prevent the copying of sensitive data to unapproved media. The solution can do it by maintaining authorized media configuration items (CIs) and maintaining white-listed media CIs.
13	**Whitelist Files and Repositories:** The solution should allow users to define a list of files and repositories that are trusted and clean files so users do not have to remediate files that are safe for distribution.	The DLP Solution will only apply the configured DLP Policies on content which is matched based on the criteria defined in the configured DLP Policy. The DLP Solution can when searching/scanning for sensitive content on network-based storage repositories or endpoints avoid scanning specific locations/repositories thereby whitelisting those locations/repositories. (Kindly confirm if our understanding is correct and therefore we can Fully comply with this requirement)	Yes.
14	The Contractor will charge the Commission a fixed amount of PKR XXX (inclusive of all taxes) for. The payment will be made as per payments terms mentioned herein after. 1. After Delivery of Licenses /Software60% 2. After Installation and Configuration20% 3. After Professional Training10% 4. After User Training10%	Please confirm that **End-User Training** (if applicable) is required and what are the locations where this training is to be given ?	End-user training may not be part of this engagement and 20% payment will be released after administrators' training
15	**Comprehensive warranty & onsite support** for mentioned years shall be given for the equipment/software/renewal at Islamabad, Karachi, and Lahore offices (if applicable).	How many sites are included in the scope of the deployment and local support? Our understanding is that the deployment of the DLP Solution is at SECP HO in Islamabad, if the deployment needs to be done at Lahore and Karachi as well kindly confirm.	The solution will be deployed at SECP, HO, Islamabad. Agent will be deployed remotely.

16	**Comprehensive warranty & onsite support** for mentioned years shall be given for the equipment/software/renewal at Islamabad, Karachi, and Lahore offices (if applicable).	Are Licenses required for 1 year or 3 years?	Initially, DLP solution's Licenses requires for 1 year
17		MDM Price quotation basis	Prices may be quoted based on exact # of users and exact # of devices. Bidder should mention the mechanism of pricing when later we wish to addition more users or devices.
18		Deployment Model	Bidder are open to participate on bids separately for On-Premises and/or On-Cloud solutions.
19		On-Premises and/or On-Cloud solutions.	Bidder are open to participate and submit bids separately for On-Premises and/or On-Cloud solutions. Top management's policy will decide whether to go for cloud or remain on-premises.
20		Infrastructure and licensing of integrated components e.g. OS, DBMS etc.	Infrastructure and licensing of integrated components are not part of these RFP scope. SECP will provide these items.
21		DLP solution's number of users	Expected number of usersof DLP solution will be approxemately **700**
22		MDM solution's number of users / number of devices	Pricing options are required for: 1. 100 Users 2. 100 Devices 3. 200 Users 4. 200 Devices 5. 300 Users 6. 300 Devices 7. Per User 8. Per Device