Financial Intelligence Unit – India

Ministry of Finance, Government of India

Project FINnet
Financial Intelligence Network

Invitation for Expression of Interest (EoI) for Hiring of Consultant

June 2006

Financial Intelligence Unit-India (FIU-IND)
6th Floor, Hotel Samrat, Chanakyapuri
New Delhi -110021, India

TABLE OF CONTENTS

1 LETTER OF INVITATION

1.1 Advertisement

1.1.1 This Expression of Interest (EoI) Document is for the Hiring of Consultant for the Project FINnet – Financial Intelligence Network. The Government of India set up Financial Intelligence Unit – India (FIU-IND) (Website: http://www.fiuindia.gov.in) on 18th November 2004 to coordinate and strengthen collection and sharing of financial intelligence through an effective national, regional and global network to combat money laundering and related crimes.

1.1.2 The objective of the Project FINnet is to "Adopt industry best practices and appropriate technology to collect, analyze and disseminate valuable financial information for combating money laundering and related crimes". The Project would consist of two phases i.e. Phase I- Preparation of the Consultancy Report and Phase II- Implementation of the Consultancy Report.

1.1.3 In the first phase, the Consultant would be responsible for preparing a detailed Consultancy Report and the in the second phase, he would act as a project manager to ensure its implementation. The Consultant is expected to have competencies in Design of Anti Money Laundering/Risk Assessment Systems, Process Design, Information Systems Design, Information Security Planning and Project Management. Consultant who is selected for preparing the Consultancy Report will be barred from participating in the bidding process for its implementation.

1.1.4 Interested bidders may download the EoI document from the website http://www.tenders.gov.in or http://www.fiuindia.gov.in/tenders or may obtain the same from FIU-IND, 6th Floor, Hotel Samrat, Chanakyapuri, New Delhi -110021, on payment of Rs. 500/- (Rupees Five Hundred only), from 9th June 2006 upto 10th July 2006 between 1000 hrs and 1700 hrs on working days. The payment will be accepted in the form of crossed demand draft drawn on any scheduled bank, payable at par in New Delhi in favour of DDO, Financial Intelligence Unit-India, New Delhi.

1.1.5 Last Date for Submission of EoI: 1500 hours (IST) on 12th July 2006.

1.1.6 You may contact Shri Sanjeev Singh, Additional Director, FIU-IND (Tel:(+91)-11-26874369, Fax:(+91)-11-26874459 Email: sanjeev.singh@fiuindia.gov.in) for any clarification.

Arun Goyal
Director, FIU-IND

1.2 Critical Information

Availability of Invitation for EoI	9th June 2006 upto 10th July 2006 between 1000 hrs and 1700 hrs on working days
Last date for receipt of Queries	1500 hours on 23rd June, 2006
Last date for receipt of EOI	1500 hours on 12th July, 2006
Time and Date of opening of EOI	1600 hours on 12th July, 2006
Place of opening of EOI	Conference Room Financial Intelligence Unit-India 6th Floor, Hotel Samrat Chanakyapuri, New Delhi -110021 India
Contact Person for queries	Sanjeev Singh Additional Director, FIU-IND Financial Intelligence Unit-India 6th Floor, Hotel Samrat Chanakyapuri, New Delhi -110021 Tel:(+91)-11-26874369, Fax:(+91)-11-26874459 Email: sanjeev.singh@fiuindia.gov.in
Contact Person for submission of EOI	O. P. Sharma Senior Technical Officer (Administration) Financial Intelligence Unit-India 6th Floor, Hotel Samrat Chanakyapuri, New Delhi -110021 Tel:(+91)-11-26874368

2 BACKGROUND INFORMATION

2.1 About FIU-IND

The Government of India set up Financial Intelligence Unit – India (FIU-IND) on 18th November 2004 to coordinate and strengthen collection and sharing of financial intelligence through an effective national, regional and global network to combat money laundering and related crimes. FIU-IND reports to the Economic Intelligence Council (EIC) headed by the Finance Minister.

2.1.1 **Organization**

FIU-IND is a multi disciplinary body with a sanctioned strength of 43 personnel. These are being inducted from different organizations namely Central Board of Direct Taxes (CBDT), Central Board of Excise and Customs (CBEC), Reserve Bank of India (RBI), Securities Exchange Board of India (SEBI), Department of Legal Affairs and Intelligence agencies. The distribution of sanctioned strength is as under:

Sl. No.	Post	Sanctioned Strength
1	Director (Group A)	1
2	Additional Director (Group A)	7
3	Technical Director (Group A)	1
4	Principal System Analyst (Group A)	2
5	Senior Technical Officer (Group A)	10
6	System Analyst/ Programmer (Group A)	3
7	Section Officer (Group B Gazetted)	1
8	PS to Director (Group B Gazetted)	1
9	P A to Addl. Directors (Group B Non-Gazetted)	8
10	Assistants (Group C)	2
11	Data Entry Operators (Group C)	2
12	Lower Division Clerk (Group C)	1
13	Peons (Group D)	4
	Total	**43**

2.2 Functions of FIU-IND

The Government of India's O.M. dated 18th November 2004 set up Financial Intelligence Unit – India (FIU-IND) as the central national agency responsible for receiving, processing, analyzing and disseminating information of suspect financial transactions to various agencies. The broad categories of functions of FIU-IND are as under:

2.2.1 **Intelligence Management**

i) Receiving reports from reporting entities.

ii) Identification of suspicious cases.

iii) Analysis of suspicious cases.

iv) Dissemination of information to relevant national intelligence/enforcement agencies and foreign FIUs.

v) Sharing information with national intelligence/enforcement agencies and foreign FIUs.

vi) Identifying and obtaining any other data/information relevant for analysis.

2.2.2 **Relationship Management**

i) Establishing and maintaining relationships with domestic intelligence/enforcement agencies, supervisory and regulatory agencies, reporting entities and foreign FIUs.

ii) Establishing membership in international organisations involved in anti money laundering efforts.

iii) Facilitating and administering MOUs with foreign FIUs.

iv) Maintaining relationships with international organisations like the IMF, World Bank, World Customs Organisation etc. to build international environment to tackle money laundering.

v) Assisting in the formulation of training programmes for reporting entities and intelligence/enforcement agencies.

2.2.3 **Policy review and development**

i) Reviewing regulatory and operational issues and suggesting policy changes.

ii) Promoting awareness on issues concerning economic crimes including money laundering.

2.3 The Prevention of Money Laundering Act, 2002

The Prevention of Money Laundering Act, 2002 (PMLA) forms the core of the legal framework put in place by India to combat money laundering. PMLA and the Rules notified thereunder came into force with effect from July 1, 2005. Director, FIU-IND and Director (Enforcement) have been conferred with exclusive and concurrent powers under relevant sections to implement the provisions of PMLA. PMLA and the Rules notified thereunder impose obligations on banking companies, financial institutions and intermediaries of securities market to verify identity of clients, maintain records and furnish information to FIU-IND. Some important sections of PMLA relevant to FIU-IND are:

- Section 1 – Short title, extent and commencement
- Section 2 – Definitions
- Section 3 – Offence of Money-Laundering
- Section 4 – Punishment for Money Laundering
- Section 12 - Obligations under PMLA
- Section 13 – Powers of the Director
- Section 14 – No civil proceedings
- Section 15 - Powers to prescribe procedure
- Section 26 - Appellate Tribunal
- Section 39 - Right of Appellant
- Section 40 – Deemed to be Public Servants
- Section 41 – Restriction on Civil Courts
- Section 42 - Appeal to High Court
- Section 44 – Offences triable by Special Courts
- Section 48 - Authorities under the Act
- Section 49 - Appointment of Authorities
- Section 50 – Summons, production of documents etc.
- Section 54 - Other authorities empowered and required to assist
- Section 56 – Agreements with foreign countries
- Section 66 - Disclosure of information
- Section 69 - Recovery of fines
- Section 75 – Power to remove difficulties

2.4 Notifications

The Central Government has issued following notifications to enforce PMLA.

Notification	Description
1/2005 dated 1st July 2005	Notified 1st July 2005 as the date on which all the provisions of PMLA shall come into force.
2/2005 dated 1st July 2005	Appointed an Adjudicating Authority to exercise jurisdiction, powers and authority conferred by or under PMLA.
3/2005 dated 1st July 2005	Notified that the New Delhi Bench of the Adjudicating Authority shall exercise jurisdiction, powers and authority conferred by or under PMLA over the whole of India.
4/2005 dated 1st July 2005	Established an Appellate Tribunal at New Delhi to hear appeals against the orders of the Adjudicating Authority and the authorities under PMLA.
5/2005 dated 1st July 2005	Conferred certain exclusive and concurrent powers under PMLA to the Director, Financial Intelligence Unit, India.
6/2005 dated 1st July 2005	Conferred certain exclusive and concurrent powers under PMLA to the Director of Enforcement.
7/2005 dated 1st July 2005	Notified Rules relating to the manner of forwarding a copy of the order of provisional attachment of property.
8/2005 dated 1st July 2005	Notified Rules for receipt and management of confiscated properties.
9/2005 dated 1st July 2005	Notified Rules for maintenance of records of the nature and value of transactions, the procedure and manner of maintaining and time for furnishing of information and verification of records of the identity of the clients of the banking companies, financial institutions and intermediaries.
10/2005 dated 1st July 2005	Notified Rules relating to the search and seizure
11/2005 dated 1st July 2005	Notified Rules relating to the arrest of a person
12/2005 dated 1st July 2005	Notified Rules relating to retention of seized property
13/2005 dated 1st July 2005	Notified Rules for the manner of receiving the records authenticated outside India.
14/2005 dated 1st July 2005	Notified Rules for the purpose of appeals under PMLA.
15/2005 dated 13th Dec 2005	Amended Rules 5, 7, 8 and 10 of Notification No. 9/2005

2.4.1 **Notification No. 5/2005 dated 1st July, 2005**

Notification number 5/2005 dated 1st July, 2005 confers following powers on the Director, FIU-IND:

> *"In exercise of the powers conferred by sub-section (1) of section 49 of the Prevention of Money-laundering Act, 2002 (15 of 2003), the Central Government hereby appoints, with effect from the 1st day of July, 2005, the Director, Financial Intelligence Unit, India, under the Ministry of Finance, Department of Revenue, as the Director to exercise the exclusive powers conferred under clause (b) of sub-section (1) of section 12 and its proviso, section 13, sub-section (2) of section 26 and sub-section (1) of section 50 of the said Act and the said Director, Financial Intelligence Unit, India, shall also concurrently exercise powers conferred by sub-section (3) and sub-section (5) of section 26, section 39, section 40, section 41, section 42, section 48, sub-section (2) of section 49, section 66 and section 69 of the aforesaid Act."*

2.4.2 **Notification No. 9/2005 dated 1st July, 2005**

Notification No. 9/2005 dated 1st July, 2005 notifies rules for maintenance of records, furnishing of information and verification of records of the identity of the clients of the banking companies, financial institutions and intermediaries. The Rules are:

- Rule 1 - Short title and commencement
- Rule 2 - Definitions
- Rule 3 - Maintenance of records of transactions
- Rule 4 - Records containing information
- Rule 5 - Procedure and manner of maintaining information
- Rule 6 - Retention of Records
- Rule 7- Procedure and manner of furnishing information
- Rule 8 - Furnishing of information to the Director
- Rule 9 - Verification of the records of the identity of clients
- Rule 10 - Maintenance of the records of the identity of clients
- Rule 11- Interpretation

2.5 Obligations under PMLA relevant to FIU-IND

Section 12 of PMLA lays down following obligations on the banking companies, financial institutions and intermediaries.

> *"12. (1) Every banking company, financial institution and intermediary shall-*
>
> *(i) maintain a record of all transactions, the nature and value of which may be prescribed, whether such transactions comprise of a single transaction or a series of transactions integrally connected to each other, and where such series of transactions take place within a month;*
>
> *(ii) furnish information of transactions referred to in clause (a) to the Director within such time as may be prescribed;*
>
> *(iii) verify and maintain the records of the identity of all its clients, in such a manner as may be prescribed*
>
> *Provided that where the principal officer of a banking company or financial institution or intermediary, as the case may be, has reason to believe that a single transaction or series of transactions integrally connected to each other have been valued below the prescribed value so as to defeat the provisions of this section, such officer shall furnish information in respect of such transactions to the Director within the prescribed time.*
>
> *(2) The records referred to in sub-section (1) shall be maintained for a period of ten years from the date of cessation of the transactions between the clients and the banking company or financial institution or intermediary, as the case may be."*

Thus there are three obligations of reporting entities under PMLA i.e. maintenance of records, furnishing information to FIU-IND and verification of identity of clients.

2.6 Maintenance of Records

Rule 3, 4, 5 and 6 of the Rules notified in Notification No. 9/2005 dated 1st July 2005 specifically provide rules for maintenance and retention of records.

2.6.1 **Maintenance of Records of transactions**

Rule 3 of the Rules notified under Notification No. 9/2005 requires every banking company, financial institution and intermediary to maintain record of –

(A) All cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency,

(B) All series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month,

(C) All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place, and

(D) All suspicious transactions whether or not made in cash.

2.6.2 **Information to be contained in Records**

Rule 4 of the Rules notified under Notification No. 9/2005 requires recording of the nature of the transactions, the amount of the transaction, the currency in which it was denominated, the date on which the transaction was conducted and the parties to the transaction.

2.6.3 **Procedure and manner of maintaining information**

Rule 5 of the Rules notified under Notification No. 9/2005 requires that every banking company, financial institution and intermediary shall evolve an internal mechanism for maintaining information in respect of transactions with its clients in hard and soft copies in accordance with the procedure and manner specified by the Regulatory agencies.

2.6.4 **Retention of Records**

Rule 6 of the Rules notified under Notification No. 9/2005 requires that the records referred to in Rule 3 shall be maintained for a period of ten years from the date of cessation of the transactions with the client.

2.7 Furnishing information

PMLA and the Rules notified thereunder require every banking company, financial institution and intermediary, to furnish to FIU-IND information relating to –

(A) All cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency,

(B) All series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month,

(C) All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place, and

(D) All suspicious transactions whether or not made in cash.

2.7.1 **Procedure and manner of furnishing information**

Rule 7 of the Rules notified under Notification No. 9/2005 lays down the procedure and manner of furnishing information. This rule requires every banking company, financial institution and intermediary to communicate the name, designation and address of it's Principal Officer to the Director, FIU-IND. This rule also requires every banking company, financial institution and intermediary to evolve an internal mechanism for furnishing information.

The Principal Officer is made responsible for furnishing the information to the Director, FIU-IND in the prescribed form.

2.7.2 **Cash Transaction Reports**

PMLA, and the Rules notified thereunder require every banking company, financial institution and intermediary, to furnish to FIU-IND information relating to –

i) All cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency, and

ii) All series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month.

The due date for furnishing cash transaction reports for a month is the 15th day of the succeeding month.

2.7.3 **Suspicious Transaction Reports**

Every banking company, financial institution and intermediary is required to furnish information of all suspicious transactions to FIU-IND. Suspicious transaction means a transaction, whether or not made in cash, which to a person acting in good faith –

i) gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or

ii) appears to be made in circumstances of unusual or unjustified complexity; or

iii) appears to have no economic rationale or bonafide purpose.

The reporting format of STR notified by RBI lays down following broad categories of suspicion for a banking company:

i) Identity of client - False identification documents; identification documents which could not be verified within reasonable time; accounts opened with names very close to other established business entities.

ii) Background of client - Suspicious background or links with known criminals.

iii) Multiple accounts - Large number of accounts having a common account holder; introducer or authorized signatory with no rationale; unexplained transfers between multiple accounts with no rationale.

iv) Activity in accounts - Unusual activity compared with past transactions; sudden activity in dormant accounts; activity inconsistent with what would be expected from declared business.

v) Nature of transactions- Unusual or unjustified complexity; no economic rationale or bonafide purpose; frequent purchases of drafts or other negotiable instruments with cash; nature of transactions inconsistent with what would be expected from declared business.

vi) Value of transactions - Value just under the reporting threshold amount in an apparent attempt to avoid reporting; value inconsistent with the client's apparent financial standing.

Similar broad categories of suspicion have been laid down by SEBI and IRDA for intermediaries of securities market and insurers respectively.

2.8 Verification of Identity of Clients

Section 12 of PMLA and the Rules notified thereunder require every banking company, financial institution and intermediary to verify and maintain the records of the identity of all its clients in prescribed manner. Rules 9 and 10 of

Notification No. 9/2005 dated 1st July 2005 provide for verification and maintenance of the records of the identity of clients.

2.8.1 Verification of the records of the identity of clients

Rule 9 of the Rules notified under Notification No. 9/2005 requires every banking company, financial institution and intermediary to verify and maintain the record of identity and current address or addresses including permanent address or addresses of the client, the nature of business of the client and his financial status. The Rule also specifies that where it is not possible to verify the identity of the client at the time of opening an account or executing any transaction, the banking company, financial institution and intermediary shall verify the identity of the client within a reasonable time after the account has been opened or the transaction has been executed. Rule 9 also specifies documents needed for verification of identity of individuals, companies, partnership firms, trusts, associations of persons or bodies of individuals.

2.8.2 Client Identification Programme

Rule 9 of the Rules notified under Notification No. 9/2005 requires every banking company, financial institution and intermediary to formulate and implement a client identification programme that it considers appropriate to enable it to determine the true identity of its clients as required under PMLA. A copy of the client identification programme is also required to be forwarded to the Director, FIU-IND.

2.8.3 Maintenance of Records of Identity

Rule 10 of the Rules notified under Notification No. 9/2005 requires every banking company, financial institution and intermediary to maintain the record of identity, current addresses, permanent address, nature of business and the financial status of the client. This rule also requires that the records of the identity of clients shall be maintained in hard and soft copies for a period of ten years from the date of cessation of the transactions with the client.

2.9 Circulars issued by Regulatory Agencies

The reporting entities under PMLA are regulated by various regulatory agencies such as:

i) Reserve Bank of India (RBI)

ii) Securities and Exchange Board of India (SEBI)

iii) Insurance Regulatory and Development Authority (IRDA)

Some significant circulars issued by the Regulatory Agencies are:

i) RBI's Circular dated 29th Nov 2004 on KYC Guidelines – AML Standards

ii) RBI's Circular dated 15th Feb 2006 on Obligation of Banks under PMLA

iii) SEBI's Circular dated 18th Jan 2006 on Guidelines for Anti Money Laundering Measures

iv) SEBI's Circular dated 20th Mar 2006 on Obligations of Intermediaries under PMLA

v) IRDA Circular dated 31st Mar 2006 on Guidelines on AML programme for Insurers

2.10 Reporting Entities under PMLA

PMLA lays down certain obligations on reporting entities falling within the definition of banking company, financial institution or intermediary. The definition of banking company, financial institution and intermediary under PMLA is given in following paragraphs.

2.10.1 **Banking Company under PMLA**

"Banking Company" under PMLA means a banking company or a co-operative bank to which the Banking Regulation Act, 1949 applies and includes any bank or banking institution referred to in section 51 of that Act. Banking Companies include:

i) All nationalized banks, private Indian banks and private foreign banks.

ii) State Bank of India and its associates and subsidiaries.

iii) All co-operative banks viz. primary co-operative banks, state co-operative banks and central (district level) co-operative banks.

iv) Regional Rural Banks.

2.10.2 **Financial Institution under PMLA**

"Financial Institution" under PMLA is defined in clause (c) of section 45-I of the Reserve Bank of India Act, 1934 and includes a chit fund company, a co-operative bank, a housing finance institution and a non banking financial company. Financial Institutions include:

i) All India Financial Institutions namely EXIM Bank, NABARD, NHB, SIDBI, IFCI Ltd., IDFC Ltd., IIBI Ltd. And TFCI Ltd.

ii) Insurance companies.

iii) Hire Purchase companies.

iv) Chit fund companies as defined in the Chit Funds Act.

v) Housing finance institutions as defined in the National Housing Bank Act such as HDFC.

vi) Non-banking financial companies such as motor and general, hire purchase companies, leasing companies, investment companies etc.

2.10.3 **Intermediary under PMLA**

"Intermediary" under PMLA includes following persons registered under Section 12 of the Securities and Exchange Board of India Act, 1992:

i) Stock brokers

ii) Sub-brokers

iii) Share transfer agents

iv) Bankers to an issue

v) Trustees to trust deed

vi) Registrars to issue

vii) Merchant bankers

viii) Underwriters

ix) Portfolio Managers

x) Investment advisers

xi) Depositories and Depository Participants

xii) Custodian of securities

xiii) Foreign institutional investors

xiv) Credit rating agencies

xv) Venture capital funds

xvi) Collective investment schemes including mutual funds

2.11 International Cooperation

The value of information exchange at an international level is very significant in combating money laundering. FIUs have an unique ability to exchange financial information that may be helpful to law enforcement investigations in following the financial trail and uncovering criminal assets.

2.11.1 **Financial Action Task Force (FATF)**

The Financial Action Task Force (FATF) is an inter-governmental body, which sets standards and promotes policies to combat money laundering and terrorist financing. The Forty Recommendations and Nine Special Recommendations of FATF provide a complete set of counter-measures against money laundering covering the criminal justice system, law enforcement, financial system regulation and international co-operation. These Recommendations have been recognised, endorsed, and adopted by many international bodies as the international standards for combating money laundering and terrorist financing.

2.11.2 **Egmont Group**

The Egmont Group serves as an international network fostering improved communication and interaction among FIUs. Egmont Group is named after the venue in Brussels where the first such meeting of FIUs was held in June of 1995. The goal of the Egmont Group is to provide a forum for FIUs around the world to improve support to their respective governments in the fight against money laundering, terrorist financing and other financial crimes. This support includes:

i) Expanding and systematizing international cooperation in the reciprocal exchange of financial intelligence information.

ii) Increasing the effectiveness of FIUs by offering training and personnel exchanges to improve the expertise and capabilities of personnel employed by FIUs.

iii) Fostering better and secure communication among FIUs through the application of technology, presently via the Egmont Secure Web (ESW).

iv) Promoting the establishment of FIUs in those jurisdictions without a national anti-money laundering/terrorist financing program in place, or in areas with a program in the beginning stages of development.

2.11.3 **Asia/Pacific Group on Money Laundering (APG)**

The Asia/Pacific Group (APG) was officially established as an autonomous regional anti-money laundering body in February 1997 at the Fourth Asia/Pacific Money Laundering Symposium in Bangkok, Thailand. The purpose of the APG is to facilitate the adoption, implementation and enforcement of internationally accepted anti-money laundering and anti-terrorist financing standards set out in the recommendations of the Financial Action Task Force (FATF). The

APG's role includes assisting jurisdictions in the region to enact laws dealing with the proceeds of crime, mutual legal assistance, confiscation, forfeiture and extradition. It also includes the provision of guidance in setting up systems for reporting and investigating suspicious transactions and helping in the establishment of financial intelligence units. The APG also undertakes studies of methods and trends of money laundering and the financing of terrorism in the Asia/Pacific region.

2.11.4 **Financial Intelligence Units**

The definition of Financial Intelligence Unit as formalised by the Egmont Group in 1996 is as under:

> *"A central, national agency responsible for receiving, (and as permitted, requesting) analysing and disseminating to the competent authorities, disclosures of financial information:*
>
> *(i) Concerning suspected proceeds of crime, or*
>
> *(ii) Required by national legislation or regulation,*
>
> *in order to combat money laundering."*

2.11.5 **Best practices for exchange of information**

Egmont Group has indicated the best practices for exchange of information between FIUs. The best practices cover areas of information exchange related to submitting request for information, processing request for information, sending reply and maintaining confidentiality. Some best practices for exchange of information between FIUs are as under:

i) All FIUs should submit requests for information in compliance with the Principles for Information Exchange that have been set out by the Egmont Group. Where applicable the provisions of information sharing arrangements between FIUs should also be observed.

ii) Requests for information should be submitted as soon as the precise assistance required is identified.

iii) When an FIU has information that might be useful to another FIU, it should consider supplying it spontaneously as soon as the relevance of sharing this information is identified.

iv) The exchange of information between Egmont FIUs should take place in a secure way. To this end the Egmont FIUs should use the Egmont Secure Web (ESW) where appropriate.

v) If necessary the requesting FIU should indicate the time by which it needs to receive an answer. Where a request is marked "urgent" or a deadline is indicated, the reasons for the urgency or deadline should be explained. All FIUs should refrain from arbitrary use of this terminology. When the requested information is only partially urgent, the request for information should use the 'urgent' mark only for the relevant sections. The requesting FIU should indicate if it desires an acknowledgment of receipt of the request. The requesting FIU may not require an acknowledgment (orally or in writing) unless the request is marked "urgent" by that FIU or, in its view, an acknowledgment is necessary in the light of the circumstances of the case. An urgent request should include the contact information for the individual responsible for sending the request.

vi) Where appropriate, especially in the case of urgent requests, and in order to speed up proceedings, the requesting FIU may ask for prior consent for further use of the information to be granted directly together with the reply itself.

vii) The Egmont Group has developed a request for information form. The use of this form should be encouraged, when exchanging information.

viii) Requests should contain sufficient background information to enable the requested FIU to conduct proper analysis/investigation.

ix) Requests shall be accompanied by a brief statement of the relevant facts known to the requesting FIU. Particular attention should be paid to:

- the information identifying the persons or companies involved (at least name and date of birth for individuals and name and registered office for companies);
- the reported suspicious or unusual transactions or activities, including the involved accounts;
- the modus operandi or circumstances in which the transactions or activities took place;
- whether the request for information is based on one or more disclosures or whether it has another base, such as a request from a national police authority, a list of suspected terrorists ;
- the link with the country of the requested FIU.

x) Requests for information that are not related to a specific country and that are being sent to several FIUs at the same time should be justified as much as possible, providing an overview of the underlying facts. Also the request should be targeted as precisely as possible. The FIU should therefore refrain from using group mailings unnecessarily and should consider carrying out preliminary research into the transactions in order to identify a possible target cluster of FIUs that are more likely to have the relevant information at their disposal.

xi) Except if indicated otherwise, all incoming requests for information originating from a counterpart FIU should be answered, also in case of a negative reply.

xii) The request should be dealt with as soon as possible upon receipt.

xiii) FIUs should assign unique case reference numbers on both outgoing and incoming case requests to facilitate tracking of a particular case request or response.

xiv) Where a request is acknowledged, the requested FIU concerned should provide the requesting unit with the name and contact details, including telephone and fax numbers, of the contact person and the case or reference number assigned to the case by the responding FIU.

xv) FIUs should give priority to urgent requests. If the receiving FIU has concerns about the classification of a request as urgent, it should contact the requesting FIU immediately in order to resolve the issue. Moreover each request, whether or not marked as “urgent”, should be processed in the same timely manner as domestic requests for information.

xvi) As a general principle, the requested FIU should strive to reply to a request for information, including an interim response, within 1 week from receipt in the following circumstances:

- if it can provide a positive/negative answer to a request regarding information it has direct access to;
- if it is unable to provide an answer due to legal impediments.

xvii) Whenever the requested FIU needs to have external databases searched or query third parties (such as financial institutions), an answer should be provided within 1 month after receipt of the request. The

requested FIU may consider contacting the requesting unit within 1 week from receipt to state that it has no information directly available and that external sources are being consulted or that it is experiencing particular difficulties in answering the request. The latter may be done orally.

xviii) If the results of the enquiries are still not all available after 1 month, the requested FIU should provide the information it already has in its possession or at least give an indication of when it will be in a position to provide a complete answer. This may be done orally.

xix) FIUs should consider establishing mechanisms in order to monitor request-related information, enabling them to detect new information they receive regarding transactions, STRs, etc. that are involved in previously received requests. Such a monitoring system would enable FIUs to inform former requestors of new and relevant material related to their prior request.

xx) Where the requested FIU desires feedback on how the information it provided was used, it should request this explicitly. When the requesting FIU is not able to obtain this information, it should reply stating the reasons why the requested feedback cannot be provided.

xxi) If appropriate, especially in case of urgent requests, and in order to speed up proceedings, prior consent for further use of the information can be granted with the reply itself.

xxii) The exchange of information between FIUs should take place in a secure way. To this end the Egmont FIUs should use the Egmont Secure Web (ESW) where appropriate.

xxiii) All FIUs should use the greatest caution when dealing with supplied information in order to prevent any unauthorized use resulting in a breach of confidentiality.

3 PRESENT STATUS

3.1 Overview

The Government of India set up Financial Intelligence Unit – India (FIU-IND) on 18th November 2004 and the Director, FIU-IND was appointed in March 2005. A core team of one Director, three Additional Directors, one Senior Technical Officer was in place at FIU-IND from November 2005. This core team at FIU-IND has completed following tasks:

i) Setting up of physical infrastructure at Hotel Samrat.

ii) Setting up of basic technical infrastructure to meet the basic functional needs of the office.

iii) Design of manual formats and data structure for reporting cash transaction reports and suspicious transaction reports.

iv) Receipt, analysis and sharing of information.

v) Development of content and design for FIU-IND website.

vi) Identification of key processes and expected outcomes for FIU-IND.

3.2 Physical Infrastructure

FIU-IND hired office space of 7127 sq. ft. in Hotel Samrat. The open hall on the 6th floor was partitioned to make office chambers, staff workspaces, conference room, library and visitor room. Fire fighting system, air conditioning system and access control system were installed to meet the operational needs of FIU-IND.

3.3 Basic Technical Infrastructure

FIU-IND has set up a basic technical infrastructure consisting of computers, LAN and local building servers to meet the basic functional needs of the office. FIU-IND intends to create a strategic plan and information system roadmap before investing in advanced technical infrastructure such as high end servers, data warehousing tools, analytical tools, gateways etc.

3.4 Reporting Formats

FIU-IND had a series of interactions with regulatory agencies and reporting entities for designing reporting formats of Suspicious/Cash Transactions Reports (STRs/CTRs). The draft reporting formats were recommended to the regulatory agencies namely RBI, SEBI and IRDA and they have already notified the manual formats and data structures for banking companies, intermediaries and insurers on 15th Feb 2006, 20th Mar 2006 and 31st Mar 2006 respectively.

3.4.1 **Reporting formats for CTR**

The manual formats for CTR consist of following forms:

i) Manual Cash Transaction Report

ii) Consolidated Report of Cash Transaction Reports

iii) Annexure A- Individual Detail Sheet

iv) Annexure B- Legal Person/ Entity Detail Sheet

In electronic reporting of CTR, the data would be extracted and submitted in six data files i.e. Control File, Branch Data File, Account Data File, Transaction Data File, Individual Data File and Legal Person/Entity Data File. Detailed

data structure, validation rules and instructions on how to extract the data files have also been notified. The Consultant will examine the data structure and manual formats during the course of this project and if necessary, updated version of the same would be notified.

3.4.2 Reporting formats for STR

The manual formats for STR consist of following forms:

i) Manual Suspicious Transaction Report

ii) Annexure A- Individual Detail Sheet

iii) Annexure B- Legal Person/ Entity Detail Sheet

iv) Annexure C- Account and Transaction Detail Sheet

The manual formats of STR notified by RBI lays down following broad categories of suspicion:

i) Identity of client - False identification documents; identification documents which could not be verified within reasonable time; accounts opened with names very close to other established business entities.

ii) Background of client - Suspicious background or links with known criminals.

iii) Multiple accounts - Large number of accounts having a common account holder; introducer or authorized signatory with no rationale; unexplained transfers between multiple accounts with no rationale.

iv) Activity in accounts - Unusual activity compared with past transactions; sudden activity in dormant accounts; activity inconsistent with what would be expected from declared business.

v) Nature of transactions- Unusual or unjustified complexity; no economic rationale or bonafide purpose; frequent purchases of drafts or other negotiable instruments with cash; nature of transactions inconsistent with what would be expected from declared business.

vi) Value of transactions - Value just under the reporting threshold amount in an apparent attempt to avoid reporting; value inconsistent with the client's apparent financial standing.

In electronic reporting of STR, the data would be submitted in six data files i.e. Control File, Branch Data File, Account Data File, Transaction Data File, Individual Data File and Legal Person/Entity Data File. Detailed data structure, validation rules and instructions on how to extract the data files have also been notified. The Consultant will examine the data structure and manual formats during the course of this project and if necessary, updated version of the same would be notified.

3.5 Receipt, Analysis and Sharing

The main function of FIU-IND is to receive cash and suspicious transaction reports, analyse these and, as appropriate, disseminate relevant financial information to enforcement and intelligence agencies. FIU-IND has already received few cash and suspicious transaction reports from reporting entities as the reporting formats were notified in Feb/March 2006. FIU-IND has also received few references from enforcement /intelligence agencies which have been accordingly analysed and shared. The Consultant will examine all the processes related to receipt, analysis and sharing of information and prepare a detailed requirement specifications for its IT enablement.

3.6 Website of FIU-IND

FIU-IND has developed and hosted its website at www.fiuindia.gov.in. The website contains information on Prevention of Money Laundering Act 2002, obligation of reporting entities, scheduled offences, notifications and publications with appropriate links between related sections. Information about related acts, related sites, downloads,

Frequently Asked Questions (FAQs) and definitions have been included to make it a comprehensive reference site on all matters related to money laundering.

3.7 Identification of Key Processes

FIU-IND has already identified some key processes and expected outcomes, which have been grouped under Intelligence Management, Relationship Management, Strategic Management, Resource Management and Technology Management. The Consultant is expected to undertake a process identification exercise as per industry best practices to further fine tune the process description and expected outcomes.

4 PROJECT OVERVIEW

4.1 Project Objective

The objective of the Project FINnet is to "Adopt industry best practices and appropriate technology to collect, analyze and disseminate valuable financial information for combating money laundering and related crimes"

4.2 Project Phases

The Project would consist of two phases i.e. Phase I- Preparation of the Consultancy Report and Phase II- Implementation of the Consultancy Report. In the first phase, the Consultant would be responsible for preparing a detailed Consultancy Report and the in the second phase, he would act as a project manager to ensure its implementation.

4.3 Phase I- Preparation of the Consultancy Report

This phase would commence within 10 days of signing of contract with the selected Consultant. In this phase, the role of the Consultant would be to study the industry best practices in each area of operation and bring in experts with relevant specialist knowledge to provide necessary inputs. The Consultant shall evolve a Strategic Plan (highlighting policy and strategic directions for FIU-IND) as well as produce a detailed Consultancy report for FIU-IND. This statement of work lists out expected outcomes in various processes such that the Consultant gets a fair understanding of the functioning of FIU-IND. However, these expected outcomes would be mapped and examined in detail by the Consultant in an iterative manner. The scope of work and the work requirements are not exhaustive and would include additional task requirements that may come up during the duration of the Project. The Consultant shall have to continuously work back and forth between the Strategic Goals (macro-view) and the expected outcomes as stated herein (micro-view) and produce a detailed Consultancy report as per industry best practices.

4.4 Phase II- Implementation of the Consultancy Report

This phase would commence with the signing of contract with the selected System Integrator(s)/vendor(s). It is clarified that the Consultant who is selected for preparing the Consultancy Report is barred from participating in the bidding process for its implementation. In this phase, the role of the Consultant would be to manage the implementation of the Consultancy Report to ensure that expected outcomes are achieved. In addition to the obligations as per this proposal, the Consultant will be required to act as honest and faithful advisors to FIU-IND in respect of all matters relating to the project and its implementation, and shall, support and safeguard the legitimate interests of the FIU-IND in any dealings with third parties or other vendors in connection with the Project.

4.5 Stakeholders

The stakeholders in FIU-IND include the employees, reporting entities, national intelligence/enforcement agencies, regulatory agencies, ministry of finance, multilateral organisations and foreign FIUs.

4.6 Challenges

The core function of FIU-IND is to receive, analyze and disseminate data. The information system of FIU-IND would integrate several software components and analytical tools to provide all functionalities in a secure, reliable and scalable manner. Some identified challenges before FIU-IND are listed below:

4.6.1 **Identification of suspicious transactions**

Under PMLA 2002, every banking company, financial institution and intermediary is required to furnish suspicious transaction reports to FIU-IND. The challenges in identification and reporting of suspicious transaction are:

i) How to develop a common understanding between the reporting entities, regulatory agencies and FIUs on what is suspicious to enable streamlined system of identification and reporting of suspicious transactions?

ii) How to encourage deployment of AML systems to assist reporting entities in detection of suspicious transactions as per common understanding in a habitual and systematic manner?

iii) How to ensure that the reporting entities capture information related to current address, permanent address, nature of business and the financial status of the client to improve the accuracy of the AML solution?

iv) How to develop a mechanism for consolidation of hot lists of criminals or terrorists which can be seamlessly integrated into the client identification module to enable identification of suspected individuals and entities?

v) How to develop a mechanism to verify the genuineness of the ID such as PAN, Passport number, Election ID card etc. quoted by a client against the database maintained by the agency which has issued the ID?

vi) How to develop a mechanism to verify the genuineness of the details of nature of business and the financial status furnished by the client for effective risk management?

FIU-IND intends to adopt best practices and set up systems to assist reporting entities in identification of suspicious transactions in a habitual manner.

4.6.2 **Receiving Reports**

Under PMLA 2002, every banking company, financial institution and intermediary is required to furnish cash/suspicious transaction reports to FIU-IND. The challenges in receiving reports are:

i) How to achieve standardised reporting formats despite differences in business and transactional data structure followed by different categories of reporting entities?

ii) How to reduce the compliance cost for the reporting entities without compromising with the data requirements for data mining and risk analysis?

iii) How to use a data quality program to monitor and improve quality of reports?

iv) How to undertake quality assurance for verifying data integrity?

4.6.3 **Analysis of Data**

One of the biggest challenge before all FIUs have been to analyse voluminous data and extract valuable information for enforcement/ intelligence agencies. Some challenges in building capacity for timely and accurate analysis of data are:

i) Which is the most appropriate methodology to:

- Identify high risk individuals, entities, accounts or transactions.
- Validate the genuineness of the IDs such as PAN quoted by a client.
- Validate the genuineness of the details furnished by the client such as address, financial status for accurate risk profiling.
- Link duplicate IDs such as duplicate PANs issued to the same person
- Match identity of persons using various parameters like name, address etc to confirm the hit and to arrive at a confidence level for each match.
- Link same person reported by several reporting entities despite variation in name and address.
- Exclude persons who match with an internal white list to reduce false positives cases.

- Maintain and update profile of reported individuals and entities to arrive at a risk score.
- Develop and update indicators which are individual characteristics that may attract attention to possible suspicious activity
- Develop and update typologies which are series of characteristics used to undertake money laundering or related crimes
- Match transaction patters with scenarios based on intrinsic knowledge, known money laundering typologies or predictive modelling techniques by ranking suspicious behaviours based on statistically derived probabilities.
- Learn from data and through learning be capable of making inferences about patterns of behaviour present in that data.
- Adapt and revise knowledge that might be applied to identify suspicious activity in accordance with the changing environment.
- Reason with incomplete information to recognize patterns of money laundering typologies.
- Dynamically create and manage business rules and alert scenarios for real-time, complex event detection and alerting.
- Detect multiple accounts and incidents of smurfing and structuring by grouping accounts based on similarity in date of opening, name of branch or transaction amount.
- Detect n-layer relationship with a suspicious individual or entity based on common address, employer employee relationship, partner firm relationship, director company relationships etc.
- Detect non-obvious relationships between individuals, entities, accounts and transactions.
- Detect inconsistencies in nature of transaction, value of transaction, activity level in account by comparing with historical data or data pertaining to similar profession or business.
- Detect and eliminate false positive cases such that no case is marked as suspicious due to data deficiencies or information gaps.
- Identify high risk cases as early as possible as value of information may be lost due to delay in detailed analysis.
- Provide explanations as to why any case is marked a suspicious which would serve as guide for risk assessment and prioritization of alerts.

ii) Which are the most appropriate software products/tools to implement the selected methodology for detection of suspicious cases and enhancing the quality of investigative case research?

iii) How to customise and integrate various software products/tools to provide an integrated solution for FIU-IND?

iv) How to develop a knowledgebase of money laundering typologies which can learn from its earlier results?

v) How to develop a mechanism to prioritise alerts generated from data analysis on the basis of identified parameters such as risk assessment, expected impact and resource availability with highest order of objectivity and transparency?

vi) How to integrate case analysis and case management tools with the underlying data and knowledgebase?

vii) How to develop strategic analytical capability to provide strategic intelligence, advice and analysis for increasing awareness and understanding of money laundering and terrorist financing, and inform the development of effective counter-strategies?

viii) How to develop a mechanism for archiving and retrieving information and data?

4.6.4 **Sharing information with other agencies**

One of the functions of FIU-IND is to disseminate and share high-quality financial intelligence to national intelligence/enforcement agencies and regulatory agencies. Some challenges in dissemination and sharing of information are:

i) How to develop an interoperability framework to enable seamless sharing of data, documents and processes with other agencies?

ii) How to develop a mechanism to facilitate exchange of information, collect additional information and track results of enquiries?

iii) How to develop a mechanism for collection of additional information from other agencies to improve the quality of analysis.

iv) How to develop a mechanism to facilitate transparent decision making on when to share, what to share and with whom to share?

v) What types of templates should be used for dissemination of information?

vi) How to ensure data privacy and confidentiality when sharing information?

4.6.5 **Miscellaneous**

Some other challenges related to FIU-IND are:

i) How to effectively use eLearning solution to educate the reporting entities about their obligations under PMLA?

ii) How to implement a compliance program to monitor and ensure compliance by the reporting entities?

iii) How to organise roles and responsibilities in FIU-IND?

iv) What should be the Key Performance measures for monitoring performance to ensure expected outcomes?

v) How to leverage public private partnership in areas involving routine and repetitive tasks to improve the efficiency and effectiveness of FIU-IND?

vi) Which technical architecture design would provide higher scalability of operations and agility to meet changing environment?

vii) How to roll out various components of information system to meet short term as well as strategic goals of FIU-IND?

viii) How to ensure foolproof confidentiality and privacy of data and information?

ix) Which security standards to be followed and for what processes?

5 TASKS TO BE PERFORMED BY THE CONSULTANT

5.1 Phase I – Preparation of the Consultancy Report

The Consultant shall perform all tasks which are necessary to prepare a detailed Consultancy Report for FIU-IND as per industry best practices. The Consultant shall at the minimum perform tasks mentioned in the subsequent paragraphs.

5.1.1 **Prepare a Project Plan**

The Consultant shall develop a Project Plan in collaboration with FIU-IND within ten days of the commencement of services that shall describe how all the elements of project management work together to ensure that scope and schedule are being managed holistically. The Project Plan developed by the Consultant shall specify the schedule of various tasks, deliverables and deployment of resources. This plan shall be submitted to the FIU-IND for review and approval. The Consultant's plan shall address at the minimum the following:

i) Description of the Consultant's organization with their proposed staffing, roles and responsibilities.

ii) Project Organization and Communication structure.

iii) Processes and tool sets to be used for quality assurance, risk management, problem resolution and other areas the Consultant deems relevant and important to the successful management of the Consultancy Project.

iv) Project plans and schedules in the form of Gantt Chart giving details of schedule of various tasks and subtasks, task durations, floats, dependencies, deliverables, milestones, resource deployment, meetings, reviews and information required from the FIU-IND.

v) Identify benchmarks for managing quality of tasks performed and acceptance criteria for the major milestones. The approved acceptance criteria will be used to determine satisfaction of milestone reviews.

vi) Security and Confidentiality practices in accordance with industry best practices to ensure the security and confidentiality of information, documents, records, software, data, reports, deliverables etc. handled during the entire Consultancy project and subsequently. It should address the succession planning with requisite checks, handover and destruction of sensitive information in case of employee changes.

vii) The Project Plan will be updated every month by monthly progress reports.

viii) The monthly progress reports will also report on test results of deliverables, quality assurance reviews and security assurance reviews with status of corrective actions and recommendations.

5.1.2 **Prepare a Strategic Plan**

The Consultant shall carry out a detailed study of the role and functions of FIU-IND, and prepare a Five Year Strategic Plan for FIU-IND (Strategic Plan 2006-2010) as per industry best practices. The Strategic Plan should be prepared in active consultation with FIU-IND and should include the mission of FIU-IND i.e. why it exists, vision of FIU-IND i.e. how does it plan to achieves its mission, values of FIU-IND, strategic sectors of FIU-IND, strategic goals of FIU-IND, performance measures to assess progress made and challenges before FIU-IND. The Consultant shall also prepare a strategic framework to visually depict interaction between strategic sectors of FIU-IND resulting in achievement of its vision and mission.

5.1.3 **Prepare a Business Vision Plan**

The Consultant shall prepare a Business Vision Plan for FIU-IND to define the set of goals and objectives at which the business modelling effort is aimed. The Business Vision document should capture very high-level objectives of a

business modelling effort. The Consultant shall identify and prioritize business processes and Business Goals. Business goals are expected to provide a basis for measuring and improving the activities of the business and thereby ensuring alignment between long-term strategic goals and short-term operational goals.

5.1.4 **Prepare a Business Use Case Model**

The Consultant shall prepare a Business Use Case Model for FIU-IND, which would be a model of the business goals of FIU-IND and its intended functions. Business Use Case defines a sequence of actions that a business performs that yields an observable result of value to a particular business actor A business actor represents a role played in relation to the business by someone or something in the business environment. The Business Use Case Model should contain brief description of the role and purpose of the Business Use Case, specification of the metrics relevant to the Business Use Case, definition of the goals of using these metrics, textual description of the workflow that the Business Use Case represents, specification of the risks of executing or implementing the Business Use Case, description of the estimated improvement potential of the Business Use Case, definition of the owner of the business process, business goals supported by the Business Use Case, relationships in which the Business Use Case participates, activity diagrams of the Business Use Case and use case diagrams showing the relationships involving the Business Use Case.

The Consultant shall also prepare a Business Analysis Model describing the realization of business use cases by interacting business workers and business entities. It would serve as an abstraction of how business workers and business entities need to be related and how they need to collaborate in order to perform the business use cases. Further, the Consultant shall prepare a business glossary to maintain a list of commonly used terms and definitions and a business rule document to capture all business rules.

5.1.5 **Prepare a Business Architecture Plan**

The Consultant shall prepare a Business Architecture Document providing a comprehensive overview of the architecturally significant aspects of the business from a number of perspectives such as Domain View, Business Process View and Organisation view. The Business Architecture Document is expected to establish a sound architectural foundation that would serve as input for defining the software architecture. The Business Architecture Document is expected to include the following:

i) Overview of the business architecture indicating major elements of the business and its environment, such as teams and external sources of influence such as reporting entities, intelligence/enforcement agencies, regulatory agencies, foreign FIUs etc.

ii) Description of the constraints and trends that could have a significant effect on the structure of the business of FIU-IND or the way in which it works.

iii) Priority sequence of business use cases on the basis of its criticality in achieving the goals of FIU-IND.

iv) High-level organization view, human resource and cultural view of FIU-IND.

v) Prioritized business use case realizations.

vi) Broad automation requirements after evaluating how new technologies can be used to make FIU-IND more effective.

vii) Description of business systems which have relatively independent capability.

viii) Description of set of responsibilities within the FIU-IND.

ix) Possible future scenario at optimal usage of the IT system and the future directions for growth.

x) Critical Success Factors which are critical for the success of the proposed system.

5.1.6 **Identify processes and key indicators**

The Consultant shall identify all key processes of FIU-IND. The Consultant shall also categorise the process into domains and core/non core category. An indicative list of processes and expected outcomes from the same is listed in later in this section. The Consultant shall perform following tasks in accordance with the COBIT (**C**ontrol **Ob**jectives for **I**nformation and Related **T**echnology) methodology for each identified process:

i) Describe the process.

ii) Define control objective of each process as to what the process intends to achieve.

iii) Define Critical Success Factors (CSF) for each process which are the most important things to do to increase the probability of success of the process. CSF should be observable and usually measurable characteristics of the organization and process and could be strategic, technological, organizational or procedural in nature.

iv) Define Key Goal Indicators (KGI) for each process that indicates whether the process has achieved its business requirements such as productivity improvements, adherence to industry standards etc.

v) Define Key Performance Indicators (KPI) for each process that determines how well the process is performing in enabling the goal to be reached.

vi) Define Maturity Models for each process, which would develop a method of scoring such that FIU-IND can grade itself from non-existent to optimized (from 0 to 5).

5.1.7 **Design the processes**

The Consultant shall design process flows for each identified process. The Consultant should ensure the following:

i) Processes are defined and aligned with the business goals of FIU-IND.

ii) Processes are scalable and their resources are appropriately managed and leveraged.

iii) People are goal-focused and have the right information on customer, on internal processes and on the consequences of their decisions.

iv) A business culture is established, encouraging cross-divisional co-operation, teamwork and continuous process improvement.

v) Control practices are applied to increase efficient and optimal use of resources and improve the effectiveness of processes.

vi) Responsibilities of executing the process, monitoring the process and modifying the process are clearly identified.

vii) Alternative processes are evaluated on the criteria of accelerating time to roll out, benchmarking performance, minimizing cost, validating feasibility, enabling scalability, providing flexibility and adapting best practices.

5.1.8 **Prepare an Information Technology Plan**

The Consultant shall prepare an Information Technology Plan for FIU-IND, which would strike an optimum balance of information technology opportunities and the business requirements. The Strategic Information Technology plan would set and manage clear and realistic expectations of what technology can offer. The Consultant should establish and apply a structured approach regarding the long-range planning process. This should result in a high-quality plan

which covers the basic questions of what, who, how, when and why. The IT planning process should take into account risk assessment results, including business, environmental, technology and human resource risks. The Consultant should consider all aspects which need to be taken into account such as the organisational model, technological evolution, costs, legal and regulatory requirements, requirements of third-parties, planning horizon, staffing, in- or out-sourcing, data, application systems and technology architectures. The IT long- and short-range plans should incorporate performance indicators and targets. The plan itself should also refer to other plans such as the organisation quality plan and the information risk management plan. The Consultant should also develop a process to modify the IT long-range plan in a timely and accurate manner to accommodate changes to the organisation's long- range plan and changes in IT conditions. FIU-IND should establish a policy requiring that IT long- and short-range plans are developed and maintained. The Consultant should ensure that the IT long-range plan is regularly translated into IT short-range plans. Such short-range plans should ensure that appropriate IT function resources are allocated on a basis consistent with the IT long-range plan. The short-range plans should be reassessed periodically and amended as necessary in response to changing business and IT conditions.

5.1.9 **Prepare an IT Organisation Plan**

The Consultant shall design an organisation structure, roles and responsibilities for the Information Technology Department in FIU-IND. The Consultant shall perform at the minimum the following:

i) Design a suitable organization structure and the manning pattern of the Information Technology Department in FIU-IND.

ii) Define roles and responsibilities for each role in the Information Technology Department.

iii) Define roles and responsibilities for each stakeholder which is critical for success of FIU-IND.

iv) Develop a policy framework with focus on human resource planning, recruitment, placement, performance evaluation, training and development.

v) Define performance characteristics and objective measurement criteria to help in implementing a policy of performance related compensation, which can take care of individual differences and at the same time, co-exist with the current system of rewards and compensation.

vi) Design a schedule for managing operations and preventive maintenance schemes.

5.1.10 **Prepare an Information Security Plan**

The Consultant should set up a system that has the means and ability to detect, record, analyze significance, report and act upon security incidents when they do occur, while minimizing the probability of occurrence by applying intrusion testing and active monitoring. The Consultant shall perform at the minimum the following:

i) Define scope of the certification by choosing specific processes depending on the strategic imperatives for information security. FIU-IND expects all its processes related to intelligence management to be compliant with international security standards such as BS7799-2.

ii) Enumerate key information assets (technology, people, processes, documents, etc.) for the critical processes within the scope.

iii) Classify the assets based on the extent to which the operation of FIU-IND would be impacted if the security (confidentiality, integrity or availability) of these assets was compromised.

iv) Carry out a risk assessment for the assets, identify threats, threat probabilities, existing vulnerabilities and arrive at a risk level.

v) Define top-level security policy specifying how the information security initiatives will be in line with organizational goals and vision.

vi) Identify controls to mitigate risks and ensure that access to the systems and data is restricted to authorized users.

vii) Document the policies and procedures to ensure implementation, monitoring, compliance and improvement of the control.

viii) Implement the controls by assigning responsibilities, determining resources required for implementation and timeframes.

ix) Complete the documentation including business continuity plan and disaster recovery plan.

x) Ensure that employees of FIU-IND have a common understanding of security requirements, vulnerabilities and threats, and they understand and accept their own security responsibilities.

xi) Define programme for identifying security baselines that have to be adhered to and enforcing security certification of staff.

xii) Define a programme for periodic third-party evaluation of security policy and its implementation.

xiii) During the project management phase the consultant is expected to conduct an internal audit of the identified processes in preparation for the certification audit.

5.1.11 **Prepare a Technical Architecture**

The Consultant should prepare a Technical Architecture to ensure consistency between information architecture, data dictionaries, applications, data syntax, classification schemes and security levels. The Consultant should design and analyze a technical architecture design which would include at the minimum the following:

i) High-level conceptual design model, which identifies the major segments or modules of the systems and application architecture including the details of data layer, application layer and the interface layer. It should represent the system components and functionality of each as determined from the analysis of business and technology problems, the various external and internal impacts, and the requirements definition.

ii) Application Portfolio, which would list out all applications or sub-systems. An indicative list of applications is as under:

- Anti-Money Laundering System to enable identification of suspicious transaction, screening of alert, prioritisation of alert, analysis of alert and reporting of suspicion.
- Extraction Transformation Loading (ETL) Tools that extracts data from various relational databases and non-relational data sources; checks data for reliability, consistency and validity, transforms as required; and loads data into the data warehouse.
- Data Warehouse and Data Marts that collect and organise data from both internal and external sources and make it available for the purpose of analysis.
- Data Mining Tools that use appropriate statistical or modeling techniques for discovery of hidden trends or rules in a large database. The system for identification of suspicious cases would include subsystems for identity matching, relationship analysis, anomaly analysis, transaction monitoring, threshold monitoring, behavioural analysis, pattern matching, risk evaluation and risk profiling.
- Adaptive Profiling Engine to store the profiles of individuals and entities.

- Rule Engine to prioritise alerts on the basis of parameters such as risk assessment, expected impact, resource availability etc.
- Data Visualization Tools that provide a visual drill-down capacity that can help examine data graphically and identify complex interrelationships.
- Online Analytical Processing (OLAP) Engine that provide ability to analyze summary and detailed information from a multi-dimensional database.
- Dashboards that provide visual representation of key information for decision making.
- Management Information Systems to enable systematic and comprehensive access to operational data for reporting based on user requirements and performance analysis. The Consultant should in consultation with the FIU-IND develop statistical reports based on common requirements of stakeholders.
- Decision Support System to perform on-line ad-hoc queries, "what if", trend, comparison, graphical, "drill-down" and other types of analysis required to provide compliance and FIU-IND's management and executive decision-making functions. The Consultant should, in consultation with FIU-IND, develop pre-defined reports that provide internal and external stakeholders with the regular summarized information based on common requirements to enable ad-hoc queries and tactical decisions.
- Electronic Document Interchange System to facilitate document digitization, indexation, storage, retrieval, transmission using best industry standards in the most resource efficient manner.
- Workflow System to enable online approval and management of the entire process of work from initial capture until archived. The workflow process should have the flexibility of being implemented with and without Electronic Document Interchange System.
- Content Management System (CMS) to ensure that content in FIU-IND is consistent, targeted and is regularly updated. The Consultant shall develop a content strategy and content management process for arraying, interacting with, representing, and displaying content. The Consultant shall make recommendations about how content should be organized, presented, and developed. The Consultant shall also develop a site map and wire frames that support the overall content strategy; define the attributes of each content type; develop representative sample content and navigational strategies. The Consultant shall also develop a content development strategy and design workflow for development and validating content of third-party content providers. The Content Management System should closely interact or be integrated with Knowledge Management System (KMS) and Learning Management System (LMS) such that content is componentized with attributes to enable effective knowledge dissemination and learning interaction.
- Knowledge Management System (KMS) to ensure capture, share, transfer and use of knowledge to enhance organizational performance. The Consultant shall assess all knowledge sources (both codified and tacit), identify the attributes of knowledge and create a classification scheme to bring consistency in storing and retrieval. The Consultant shall develop a plan for capture and exchange of tacit knowledge. The Knowledge management System should support collaboration between users such that users can locate experts based on the profiles maintained and then interact to exchange knowledge with these experts. The Knowledge Management System should closely interact or be integrated with Content Management System (CMS) and Learning Management System (LMS) for effective codification and dissemination of knowledge.
- Learning Management System (LMS) to assess the training needs, prepare courses, suggest appropriate course and evaluate performance of the target segment, which would include the reporting entities, partners and employees of FIU-IND. The LMS would use appropriate blend of training methods such as distributable print media, distributable electronic media, online learning (e-learning) content, e-tutoring, e-coaching, e-mentoring, asynchronous online collaborations (email, bulletin boards), synchronous online

collaborations (chat, application sharing, audio conferencing, video conferencing, virtual classrooms), online knowledge management systems (searching knowledge bases, data mining, document and file retrieval, ask an expert) and internet access (search engines, websites, user groups). The LMS should be compatible with international standards (SCORM, IMS) and integrated with Content Management System, Knowledge Management Systems and collaboration platform of FIU-IND. The LMS should also be integrated with the Electronic Gateway such that upload error reports and data quality program should trigger pushing of relevant training material to the reporting entity.

- Communication System to ensure transmission, receipt, collection, aggregation, reporting and display of communications. The Communication System should link external email to internal communication system, segregate official and personal communication, integrate communication with SMS, Chat, tele and Video conferencing, standardize any and all inputs into a single, uniform format to enable workflow management for routing, processing and storing data.

iii) Technical architecture to include computers, operating systems, middleware, networks, telecommunication links, storage technologies etc. The functional view of the technical architecture should include server locations, methods of communication between collection devices and servers, network infrastructure, network data load per transaction etc.

iv) Data architecture to provide a framework for the information needs of FIU-IND including data objects and relationship between them. The Consultant should also specify clear allocation of data ownership. The data structure for reports should attempt to reduce compliance cost for the reporting entities and should also meet the data requirements for data mining and risk profiling.

v) Application architecture encompassing all elements of a system that transform objects within data architecture, which would include applications, software and also role of information providers, transformers and consumers.

vi) Security Architecture to mitigate risks and ensure that access to the systems and data is restricted to authorized users. The security architecture should include Intrusion Prevention System, Intrusion Detection System, Firewall and Anti-virus distribution.

vii) Service Delivery Framework to ensure secure, reliable and scalable delivery of service.

viii) Interoperability Framework to enable sharing of data, documents and processes with partners and stakeholders.

ix) Business Continuity Plan and Disaster Recovery Plan to handle disasters and other risks.

5.1.12 **Prepare a Technology Evaluation Report**

The Consultant shall evaluate technologies and products to analyse alternative opportunities measured against user requirements. The evaluation should be based on soundness of design, robustness of functionality, operability, integration, performance, scalability, acceptability, support and sustainability. The Consultant should preferably use proven technology as a matter of principle and new technology only where needed, justified by a business case. The Consultant should recommend most appropriate products or solutions saving time on software selection by focusing on the best of breed. During the systems integrator(s)/vendor(s) selection stage, the Consultant shall assist FIU-IND in evaluation of vendor such that appropriate vendor is selected. The Consultant should assist FIU-IND in judicious hardware acquisition, assessment of hardware and software performance, consistent system administration and ease of integration across different technology platforms.

5.1.13 **Prepare an Implementation Plan**

The Consultant shall prepare a detailed phased implementation plan in context with the overall priorities of FIU-IND with respect to time, resources and investment outlays. The Consultant should prepare a detailed implementation roadmap, which would include at the minimum the following:

i) Define an implementation approach containing different phases of the pilot and full-scale implementation of the IT system.

ii) Define an implementation time frame and complete system rollout plan based on proposed schedule implementation time frames.

iii) Identify the scope of all relevant industry standards and certifications for quality management and quality assurance.

iv) Prepare an estimated implementation cost for each identified phases of the project. The budgetary estimate will include development, hardware, software, storage, networking, WAN connectivity, roll out, training, etc. cost which is necessary for successful implementation of each identified phases of the project.

v) Prepare testing and product acceptance plans, which would be used to test the deliverables submitted by the implementing vendors including the systems integrator.

vi) Prepare a training plan for FIU-IND as well as stakeholders including training approach, methodology, and schedule for technology know-how transfer to the users of this system. The Consultant will work jointly with FIU-IND in planning and spelling out the training needs, content of training and the number of persons attending the training.

vii) Prepare a flexible and adaptable change management plan to transition users at all levels of the hierarchy to the new working environment. This shall include at least to identify communication mediums and forums preferred by the stakeholders; communicate clearly, concisely and often the anticipated changes; help the stakeholders through the transition; provide details of and address changes at individual stakeholder levels; clearly articulate the measures to mitigate adverse affects of the proposed changes. The change management plan should secure the buy-in of each employee so that everyone clearly understands “What will this change mean to me?"

viii) Prepare a communications and media plan to include all activities, which affect the brand image of the FIU-IND and education of reporting entities and partners.

5.1.14 **Preparation of Request for Proposals (RFPs)**

The Consultant shall be fully responsible for requirement anticipation (foreseeing system requirement based on previous experience), requirement investigation (study and documentation of the proposed system) and requirement specification, which would describe the operational details, performance criteria and strategies to achieve the stated requirements. The Consultant shall prepare all the functional requirement specifications (FRS) and non-functional requirements (NFRs) such that implementing vendor(s) do not again require additional inputs from FIU-IND. The functional requirements should describe the behaviours (functions or services) of the system that support user goals, tasks or activities and non-functional requirements should include all constraints and qualities. The document prepared by the Consultant should also include the Use-Case Specifications which contain the role and purpose of the use case. The use case describes what happens inside the system, what the actor does and what the system does in response. The Consultant should also document the goal to be achieved by use case, list of actors involved in the use case, conditions that must be true for use case to terminate successfully, interactions between actors and system necessary to achieve goal and any variations in the steps of a use case.

The requirement specifications shall be prepared as per industry best practices and would also include process definition, process objective, process stakeholders, process activities, tasks, activity owners, job owners, process owners, process triggers, process flows, functional flows, workflow diagrams, sequence diagrams, data/ information requirements, process performance measures, interfaces, form designs, MIS reports, role responsibilities, operating requirements and lifecycle requirements. Requirements for software development should be modular with each process or group of processes designed in such a manner that they can be approved and implemented independently as far as possible.

The Consultant shall be responsible for the assessment of work and effort required in the specified work area and also give an budget estimate for implementation. The Request For proposal (RFP) for identification of vendor(s) should contain at the minimum scope of work, instructions to the vendor, content of the bid, evaluation matrix, timeline, payment schedule and general conditions of contract. The Consultant should prepare RFP for selection of Systems Integrator(s)/vendor(s) to perform following areas of work:

i) Integrate software products with technical infrastructure to provide a customised solution to FIU-IND.

ii) Develop and maintain interfaces for FIU-IND such as Website or Interactive Voice Response System etc.

iii) Impart user training of the new information system.

iv) Capture data from manual documents and registers into electronic format to ensure that complete data is available in the new information system at the time of roll out.

v) Provide managed assured services to FIU-IND.

vi) Set up or manage Document Management System.

vii) Provide asset management service, facility management service and other contracts for annual maintenance.

viii) Test information system components as per testing plans.

The above responsibilities are only indicative and the Consultant would list out responsibilities which are necessary for the successful implementation of the Consultancy Report. The Consultant would also suggest aggregation or segregation of responsibilities as deemed necessary.

5.2 Phase II- Implementation of the Consultancy Report

In this phase, the role of the Consultant shall be to manage the project and ensure its successful implementation. The Consultant would ensure that information system, people and infrastructure are aligned as per detailed requirements specified in the Consultancy Report.

5.2.1 **Manage the Project Implementation**

The Consultant shall set up a program management office in FIU-IND and perform all functions necessary to support both program- and project-level responsibilities, which would include at the minimum the following:

i) Use best practices for program management, quality assurance, configuration management, risk management, problem resolution, subcontractor management, and other areas the Consultant deems relevant and important to the successful management of the implementation.

ii) Identify performance measures that will be used to determine the overall performance of the vendors.

iii) Conduct preliminary assessment of all project risks (associated with the technical aspects of the work to achieve require outcomes) or process risks (associated with the project processes, procedures, tools, controls and techniques employed) and risk mitigation strategies.

iv) Ensure that resources are available to support a separate test environment and sufficient time is allowed for the test process.

v) Coordinate with the vendors to ensure the completeness and correctness of requirement specifications.

vi) Ensure that test data is available and representative of live data in kind and quantity, and the test environment reflects as close as possible the live environment.

vii) Supervise testing and acceptance of all components of information system including hardware and software in accordance with the testing and product acceptance plan.

viii) Review user training manuals developed by vendors.

ix) Update the project plan and timeline.

5.2.2 **Assist in Validation of Requirements**

The Consultant shall assist the selected implementing vendors in explaining the requirement specifications and modify the same, if required, to ensure successful implementation. The Consultant should ensure that the implementing vendor(s) validate the adequacy and sufficiency of the requirement specifications.

5.2.3 **Knowledge Transfer**

The Consultant shall be responsible for complete knowledge transfer to FIU-IND through a systematic knowledge transfer plan to ensure effective implementation and continuous improvement.

6 EXPECTED OUTCOMES

The purpose of this section is to give an indicative list of processes and expected outcomes such that the Consultant gets an insight into the role and functions of FIU-IND. The final list of processes and expected outcomes would be determined during the Consultancy project in an iterative manner. As mentioned earlier, the Consultant shall prepare a Strategic Plan for FIU-IND which would include the mission, vision, values, strategic sectors and strategic goals for FIU-IND. Some broad expectations of FIU-IND are as under:

i) Deter money laundering and related crimes.

ii) Timely and accurate detection of money laundering.

iii) Low compliance cost for reporting entities.

iv) Disseminate valuable financial intelligence.

v) Coordinate with other agencies to combat money laundering.

vi) Promote professional excellence and adopt industry best practices.

vii) Increase organizational agility and flexibility.

6.1 Intelligence Management

Intelligence Management would cover all processes related to collection, handling, analysis and dissemination of intelligence.

6.1.1 **Allotment of unique ID for Reporting entities**

This process would enable allotment of unique ID to reporting entities. The process should achieve at the minimum the following:

i) Enable submission of application from reporting entities in both electronic and manual format.

ii) Enable tracking of application and reporting delays.

iii) Enable submission of changes in application details.

iv) Enable allotment of a unique ID for the reporting entity which can be used as an ID for PKI infrastructure.

v) Enable verification of genuineness and accuracy of application details.

vi) Eliminate and prevent allotment of duplicate IDs to one reporting entity.

vii) Enable certain changes to the details of reporting entity over the Internet, using a Personal Identification Number (PIN), a digital signature or other electronic authentication.

viii) Enable logging of changes and interactions to ensure quality and accuracy of data.

6.1.2 **Receiving reports from reporting entities**

This process would enable receipt of prescribed reports from reporting entities in a secure and reliable manner. The process should achieve at the minimum the following:

i) Enable filing of prescribed reports such as Cash Transaction Report, Suspicious Transaction Report, Counterfeit Currency Report both in paper and electronic format.

ii) Increase the percentage of reports filed in electronic form.

iii) Reduce the low compliance cost for reporting entities.

iv) Enable ease of preparation, less ambiguity, in-built validation checks and ease of data entry.

v) Enable lower report preparation costs by increasing alignment of data structure of reports with the transactional data maintained by the reporting entities.

vi) Enable both online and offline return preparation.

vii) Enable pre-validation to eliminate errors.

viii) Enable bulk filing of report.

ix) Enable processing of reports and issue of acknowledgement.

x) Enable identification of errors and deficiencies and its resolution within a reasonable timeframe.

xi) Enable reporting entity to obtain status of report processing.

6.1.3 **Identification of suspicious cases**

This process would enable identification of suspicious transactions, individuals, entities from available reports, data, information and risk profiles using sophisticated data mining and analytical tools. The process should achieve at the minimum the following:

i) Enable identification of suspicious individuals and entities by matching it with an internal hot list which will be compiled from a variety of sources such as OFAC's Specially Designated Nationals, Blocked Persons List, United Nations Consolidated List, Terrorist Exclusion List, Bank of England Consolidated List, Bureau of Industry and Security List, CBI List, World Check etc.

ii) Enable identity matching using various parameters like name, address etc to confirm the hit and to arrive at a confidence level for each match.

iii) Enable exclusion of persons who match with an internal white list to reduce false positives cases.

iv) Enable profiling of individuals and entities by defining profiling rules to arrive at a risk score.

v) Enable monitoring of transactions to identify out suspicious transaction patterns using advanced data mining techniques such as behaviour analysis, relationship analysis, pattern analysis, predictive analysis, cluster analysis, anomaly analysis, association analysis etc.

vi) Enable maintenance and updation of indicators which are individual characteristics that may attract attention to possible suspicious activity

vii) Enable maintenance and updation typologies which are series of characteristics used to undertake money laundering or related crimes

viii) Enable matching with scenarios based on intrinsic knowledge, known money laundering typologies or predictive modelling techniques by ranking suspicious behaviours based on statistically derived probabilities.

ix) Enable learning from data and through learning be capable of making inferences about patterns of behaviour present in that data. This would involve development of suitable risk profiling algorithms for different types of money laundering typologies related to placement, layering or integration stages of money laundering.

x) Enable adaptation and revision of the knowledge that might be applied to identify suspicious activity in accordance with the changing environment.

xi) Enable identification of patterns for placement techniques such as Smurfing and Structuring where multiple deposits in multiple accounts to avoid detection and reporting, single upfront payment for insurance, alternative remittances and electronic transfers.

xii) Enable identification of patterns for layering techniques such as movement of funds through offshore banks, shell corporations, trusts, walking accounts or intermediaries.

xiii) Enable identification of patterns for integration techniques such as business loan from shell corporation, equity investment by shell corporation, transfer of asset at a deflated/inflated price, mixing illegal funds with cash flow of a seemingly legitimate cash –intensive business, over-invoicing of exports, under-invoicing of imports or manipulated share transaction to show fictitious profits in shares.

xiv) Enable reasoning with incomplete information to recognize patterns of money laundering typologies.

xv) Enable dynamic creation and management of business rules and alert scenarios for real-time, complex event detection and alerting.

xvi) Enable detection of multiple accounts and incidents of smurfing and structuring by grouping accounts based on similarity in date of opening, name of branch or transaction amount.

xvii) Enable detection of n-layer relationship with a suspicious individual or entity based on common address, employer employee relationship, partner firm relationship, director company relationships etc.

xviii) Enable identification of inconsistencies in nature of transaction, value of transaction, activity level in account by comparing with historical data or data pertaining to similar profession or business.

xix) Enable identification and elimination of false positive cases such that no case is marked as suspicious due to data deficiencies or information gaps.

xx) Enable identification of common mistakes and provide this information to educate reporting entities about potential errors in reporting.

xxi) Enable explanations as to why any case is marked a suspicious which would serve as guide for risk assessment and prioritization of alerts.

6.1.4 **Screening and Prioritisation of suspicious cases**

This process would enable screening and prioritisation of suspicious cases generated from data mining/analytical tools, Suspicious Transaction Reports received from reporting entities and references received from national intelligence/enforcement agencies. The process should achieve at the minimum the following:

i) Enable prioritisation of suspicious cases on the basis of risk analysis score, expected impact and resource availability.

ii) Enable selection of appropriate analysis method and analysis tool.

iii) Enable selection of appropriate personnel to analyse the suspicious case.

iv) Ensure transparency, fairness and equity in screening and prioritisation of suspicious cases.

6.1.5 **Analysis and Reporting of suspicious cases**

This process would enable analysis and reporting of suspicious cases. The process should achieve at the minimum the following:

i) Enable linking of all relevant information available with FIU-IND, which could be relevant for risk analysis.

ii) Enable linking of related transactions, accounts, persons and entities to present a comprehensive view.

iii) Enable visual representation and temporal analysis of transactions, accounts, persons and entities.

iv) Enable review of relationships to remove insignificant relationships.

v) Enable access to a knowledgebase containing typologies and patterns of money laundering.

vi) Enable access to profiles maintained for each individual or entity.

vii) Enable collection of additional information from external sources relevant for analysis.

viii) Enable case management capabilities with inbuilt workflow management and reporting.

ix) Enable a system where minimum standard verifications of selected issues are completed.

x) Enable preparation of report in a template for the national intelligence/enforcement agencies or regulatory agencies containing nature of suspicion, related individuals, related entities, related transactions and related accounts.

6.1.6 **Obtaining external data or information relevant for analysis**

This process would enable obtaining external data or information to improve the quality of analysis. As per best practices for the exchange of information between financial intelligence units, FIUs should have speedy access to all relevant tools and registers existing in their respective jurisdiction, including law enforcement information; information held by financial institutions and other reporting entities; and information on beneficial ownership and control of legal persons, such as corporate entities and trusts. The process should achieve at the minimum the following:

i) Enable identification of relevant information available with external agencies, which could be relevant for risk analysis.

ii) Enable sending request for obtaining external data or information.

iii) Enable receipt of external data or information.

iv) Enable linking of received information with could be relevant for risk analysis.

6.1.7 **Sharing information**

This process would enable seamless exchange of data, process and metadata with national intelligence/enforcement agencies, regulatory agencies and foreign FIUs. The process should enable an Interoperability framework, which would contain common standards for facilitating seamless exchange of data, process and metadata in a secure manner. The process should also ensure higher accuracy, standardization and reliability of collected information. The sharing of information from FIU-IND to Intelligence/enforcement agencies would include dissemination of relevant financial information after analysis of reported data and providing information on request in connection with investigation of scheduled offences under PMLA. Other agencies would send alerts on suspicious transactions and give feedback on information disseminated by FIU-IND.

6.1.8 **Document Management**

This process would enable efficient receipt, storage, retrieval and transfer of records for maintenance of existing and future paper records or documents based on industry best practices. The process should enable proper receipt and handling of records, systematic and secure storage of records, faster and accurate retrieval of records on request, guaranteed dispatch of records to authorized users, tracking and linking related documents or records pertaining to a case and regular weeding out of records.

6.2 Relationship Management

The processes under relationship management would ensure that FIU-IND maintains relationships with reporting entities, national enforcement /intelligence agencies, regulators and foreign FIUs.

6.2.1 **Education of reporting entities**

This process would enable education of reporting entities. The process should achieve at the minimum the following:

i) Provide updated information on PMLA, Procedures, Forms and Publications through various media such as website, e-mail using the Content Management System (CMS)

ii) Target reporting segments based on specific needs and awareness levels using the Learning Management System (LMS).

iii) Enable fast and easy search and retrieval of information.

iv) Enable knowledge based support for clarifications.

v) Receive inquiries from a variety of media, including e-mail, e-forms, fax, post, telephone and in-person.

vi) Provide high quality, accurate responses to inquiries the first time the inquiry is received.

vii) Enable a help desk facility, which provides first-line support and advice.

viii) Provide skill-based routing of inquiries.

ix) Enable reporting entities to contact FIU-IND staff in an escalation strategy - first by e-mail, then voice and finally in person based upon the complexity of the situation.

x) Enable queue management supported by workflow management to track the status of inquiries.

xi) Maintain and update checklists, FAQs, step- by-step guide etc to increase awareness and resolve queries.

6.2.2 **Ensuring compliance of Reporting entities**

This process would enable FIU-IND to ensure compliance of reporting entities to their obligations under PMLA such as appointment of principal officer, verifying the identity of clients, maintaining records and furnishing information to FIU-IND. The process should achieve at the minimum the following:

i) Track compliance of reporting entities.

ii) Select reporting entities who have not complied with the obligations under PMLA.

iii) Select the appropriate compliance action such as sending letter, education material, imposing fine etc depending on nature of default, frequency of default or other identified parameters.

iv) Track the compliance action to its logical end to ensure compliance.

6.2.3 **Maintaining relationship with National Intelligence/Enforcement Agencies**

This process would enable maintaining relationship with national intelligence/enforcement agencies. The process should achieve at the minimum the following:

i) Capture the details of nodal officers.

ii) Decide on data and information to be shared.

iii) Establish procedures for data sharing.

iv) Identify areas of cooperation and assistance.

6.2.4 **Maintaining relationship with Regulatory Agencies**

This process would enable maintaining relationship with regulatory agencies. The process should achieve at the minimum the following:

i) Capture the details of contact persons.

ii) Decide on data and information to be shared.

iii) Establish procedures for sharing alerts and information.

iv) Identify areas of cooperation and assistance.

6.2.5 **Maintaining relationship with International Organizations**

This process would enable FIU-IND in getting membership of multilateral organisations and become part of international effort to combat money laundering.

6.2.6 **Maintaining relationship with Foreign FIUs**

This process would enable FIU-IND in signing agreements with financial intelligence units to enable sharing of information.

6.2.7 **Technical assistance and cooperation**

This process would enable FIU-IND in identifying areas of common interest and ensure technical cooperation with national enforcement /intelligence agencies, regulators and foreign FIUs.

6.3 Strategic Management

The processes under strategic management would give strategic direction to FIU-IND to ensure that it plays a significant role in combating money laundering.

6.3.1 **Monitoring money laundering trends and developments**

This process would enable monitoring of money laundering trends and patterns. The process should achieve at the minimum the following

i) Monitor money laundering trends and methods.

ii) Publish sanitised cases and money laundering typologies to increase awareness about money laundering.

iii) Suggest policy changes to counter money laundering.

6.3.2 **Evaluation of outcomes in accordance with Strategic Plan**

This process would enable evaluation of outcomes achieved by FIU-IND and compare it with the Strategic Plan. This would enable FIU-IND to publish an annual account of performance against expected performance.

6.4 Resource Management

The processes under resource management would ensure that right resource i.e. people and infrastructure is made available at the right time to achieve expected outcomes.

6.4.1 **Training and Learning Management**

This process would train the employees and establish an environment for a learning organization at FIU-IND. The process should achieve at the minimum the following:

i) Identify competencies required for each job in the new working environment.

ii) Develop and manage training material for each competency and skill level.

iii) Evaluate competencies of each employee.

iv) Design training schedules for employees as per competency gaps

v) Measure the results of training and modify training strategy.

vi) Establish an environment for a learning organization that encourages innovation and on going process improvement.

vii) The training process would be enabled on a Learning Management System (LMS), which should be compatible with international standards such as SCORM, IMS etc.

6.4.2 **Performance Management**

This process would enable measurement of performance of all employee of FIU-IND. The performance measurement and appraisal systems should achieve at the minimum the following:

i) Objectivity of measurement.

ii) Congruence between individual performance and performance measurement.

iii) Congruence between performance measurement and organizational goals.

iv) Congruence with incentive structures for higher motivation.

6.4.3 **General Administration**

This process would enable an efficient general administration covering areas such as payroll management, service record management, reimbursement of expenses, requisition of consumables, budgeting and procurement etc.

6.4.4 **Infrastructure Management**

This process would enable management of infrastructure including all assets and facilities used by FIU-IND. The process should enable maintenance of inventory of asset owned by FIU-IND including computers, printers, equipments etc and its updating. This process should also result in effective management of facilities used by FIU-IND.

6.5 Information Technology Management

The information system would support business outcomes and support future requirements. The Information System modules would include following minimum components:

i) Seamless Transaction Processing System to reduce multiple data entry, increase accuracy and allow offline data entry.

ii) Reconciliation Mechanism to handle deficient or imperfect data.

iii) Workflow system to ensure that work is pushed to authorised persons habitually.

iv) Escalation system to ensure that instances of delays are escalated to superiors for intervention.

v) Collaboration platform to involve all available talent in FIU-IND.

vi) Management Information System to generate all statistical reports.

vii) Decision Support System to assist decision-making and evaluate impact of decisions.

6.5.1 **Information Security Management**

This process shall address the methodologies, processes, and systems to be used in managing various risks. The process shall include at the minimum the following:

i) Provide a security against unauthorized access at the data item, record, database and transaction level.

ii) Provide a secure, fast, reliable, intrusion free link between the intranet and the Internet or extranets to provide access to the internet or allow gateways for exchange of data and information.

iii) Enable intrusion prevention and detection systems to ensure the security and privacy of data.

iv) Enable virus management strategy to prevent and detect virus attacks.

v) Ensure compliance with approved accreditation documentation such as BS 7799-2.

vi) Control and secure application programs and system software from tampering or unauthorized access.

vii) Limit access to ad-hoc report generation programs to authorized users only.

viii) Enable backup and recovery procedures for functionality and data.

6.5.2 **Incident Management**

This process would enable a incident management system which records and tracks all abnormal incidents at FIU-IND. The process shall include at the minimum the following:

i) An accurate means of communicating problem incidents, symptoms, diagnosis and solutions to the proper support personnel is in place.

ii) Accurate means exist to communicate to users and IT the exceptional events and symptoms that need to be reported to problem management.

iii) Training is provided to support personnel in problem resolution techniques.

iv) Up-to-date roles and responsibilities charts are available to support incident management.

v) Post-facto analysis of problem handling procedures is applied.

vi) There is clear integration of problem management and change management.

vii) Accessibility to configuration data, as well as the ability to keep track of problems for each configuration component.

6.5.3 Software Development, Testing and Product Acceptance

This process would ensure that technical features of software meet the business requirements at the shop floor. The process shall include at the minimum methodologies for the following:

i) Identification of need.

ii) Listing of functional and non-functional requirements.

iii) Identification of software developer.

iv) Evaluation of software developer.

v) Changing the requirements.

vi) Testing and acceptance of software.

6.5.4 Configuration Management

This process would ensure identification and regular verification of all IT assets and their physical location. The process shall ensure at the minimum the following :

i) Owners are established for all configuration elements and are responsible for maintaining the inventory and controlling change.

ii) Configuration information is maintained and accessible, based on up-to-date inventories and a comprehensive naming convention.

iii) An appropriate software library structure is in place, addressing the needs of development, testing and production environments.

iv) There exists a release management policy and a system to enforce it.

v) Record keeping and physical custody duties are kept segregated.

vi) Vendor catalogues and configuration are aligned.

vii) Configuration baselines exist, identifying the minimum standard components and integration requirements, consistency and integration criteria.

viii) There is zero tolerance for illegal software.

6.5.5 Third-party Services Management

This process would ensure review and monitoring of existing agreements and procedures for their effectiveness and compliance with the organization policy. The process shall ensure at the minimum the following:

i) Clearly-defined service requirements and performance measures exist.

ii) The organization retains accountability and control, and proactively manages external services.

iii) The service provider has a mechanism in place to report on performance measures.

iv) Third-party providers have a quality assurance programme in place.

v) All deliverables, including operational and performance requirements, are sufficiently defined and understood by all parties.

vi) Contracts are subject to successful legal review and sign-off.

vii) There is provision for adequate management and administration, addressing financial, operations, legal and control issues.

viii) The application of mutually agreed service level agreements is based on agreed upon associated rewards and penalties.

ix) An internal contract manager is the single point of contract with the third party.

x) A process is in place for classifying service problems based on their importance and the required responses.

6.5.6 **Data Management**

This process would enable effective combination of application and general controls over the data and operations. The process shall ensure at the minimum the following:

i) Data entry requirements are clearly stated, enforced and supported by automated techniques at all levels, including database and file interfaces.

ii) The responsibilities for data ownership and integrity requirements are clearly stated and accepted throughout the organization.

iii) Data accuracy and standards are clearly communicated and incorporated into the training and personnel development processes.

iv) Data entry standards and correction are enforced at the point of entry.

v) Data input, processing and output integrity standards are formalized and enforced.

vi) Data is held in suspense until corrected.

vii) Effective translation of data across platforms is implemented without loss of integrity or reliability to meet changing business demands.

viii) There is decreased reliance on manual data input and re-keying processes.

ix) Efficient and flexible solutions promote effective use of data.

x) Data is archived and protected and is readily available when needed for recovery.

6.5.7 **Data Quality Management**

This process would enable effective management over data quality. The process shall ensure at the minimum the following:

i) Identify data flows in all processes where receipt of deficient or inaccurate data is possible or already exists.

ii) Assess the impact of deficient data or information gap.

iii) Strategy to minimize data deficiencies, which would include format validation or validation of key data fields.

iv) Strategy to eliminate or substantially reduce data deficiencies in existing data and also on an ongoing basis.

v) Enable deficient data reconciliation as a part of every process wherever applicable.

vi) Enable data certification to ensure accurate data is certified by process owners.

6.5.8 System Confidence Validation

This process would improve confidence in systems by its continuous validation by internal and external auditors. The process should achieve at the minimum the following:

i) Conduct audit of procedures and systems to locate errors or areas for concern.

ii) Identify cases where similar errors may have occurred.

iii) Suggest remedial action to be taken.

iv) Track remedial action to ensure that it is completed in reasonable time.

v) Suggest changes to procedures to reduce similar mistakes.

vi) Prepare and revise checklist based on best practices to improve quality.

vii) Improve confidence in the system operations.

6.5.9 Quality and Certification Management

This process would enable adoption of appropriate quality standards and propagate a formal system for quality management. The process should achieve at the minimum the following:

i) Determine and formally create QMS.

ii) Prepare written documents and the established QMS and then records facts as evidence.

iii) Put the QMS into action for achieving compliance to the appropriate quality standard.

iv) Maintain processes in proper or good condition such that the organization retains the achieved standards.

v) Constantly strive to improve on the existing levels by moving ahead, ‘in small but regular improvement steps’.

6.5.10 Continuous Process Improvement

This process would create a learning organization, which would encourage individual initiative, sharing of ideas, innovation and improvements on a continuous basis. The process should achieve at the minimum the following:

i) Enable Six Sigma methodology based on DMAIC process: define the problem, measure the defects and process operation; analyze the data and discover cause of the problem; improve the process to remove causes of defect; and control the process to make sure defects do not recur.

ii) Enable capture of ideas, innovation and improvements on a continuous basis.

iii) Enable systematic evaluation of ideas, innovation and improvements.

iv) Enable communication of reasons of non acceptance, if any.

7 TIMELINE AND DELIVERABLES

7.1 Broad Timeline

The broad timeline for this Project is as under:

Project Phase	Commencement date	Expected completion date
Phase I – Preparation of the Consultancy Report	Within 10 days of signing of contract with the selected Consultant	Six months from the date of commencement of Phase I.
Phase II- Implementation of the Consultancy Report	Date of signing of contract with the selected System Integrator(s)/ vendor(s)	Six months from the date of commencement of Phase II.

If more than one System Integrator are selected for the implementation, Phase II will commence from the date of signing of contract with the first System Integrator.

7.2 Milestones and Payment Schedule

The Payment schedule would be linked to following milestones:

Milestones	Percentage	Cumulative	Expected Date
Project Plan	10	10	1 months from the commencement of Phase I
Business Architecture Plan	20	30	2 months from the commencement of Phase I
Consultancy Report	25	55	5 months from the commencement of Phase I
RFP for selection of vendors	15	70	6 months from the commencement of Phase I
Implementation milestones would be decided during implementation planning	30	100	Within 6 months from the commencement of Phase II

7.3 List of Deliverables

The Consultant may propose other deliverables and work products deemed necessary or appropriate. Using the list provided in the following table and expanding on it to include other deliverables/ work products, the Consultant shall propose the set of deliverables and work products deemed necessary to conduct this task order and also propose due dates keeping in view the overall time line as described above. The following table identifies, at a minimum, some such deliverables.

S.No.	Deliverables	Refer Para	Due Date
1	Project Plan	5.1.1	10 days from date of commencement
2	Strategic Plan	5.1.2	TBN*
3	Business Vision Plan	5.1.3	TBN*
4	Business Use Case Model	5.1.4	TBN*
5	Business Architecture Plan	5.1.5	TBN*

6	Processes and key indicators	5.1.6	TBN*
7	Designed Processes	5.1.7	TBN*
8	Information Technology Plan	5.1.8	TBN*
9	IT Organisation Plan	5.1.9	TBN*
10	Information Security Plan	5.1.10	TBN*
11	Technical Architecture	5.1.11	TBN*
12	Technology Evaluation Report	5.1.12	TBN*
13	Implementation Plan	5.1.13	TBN*
14	Request for Proposals (RFPs) for Vendor Selection	5.1.14	TBN*
15	Project Implementation	5.2.1	TBN*
16	Validation of requirements	5.2.2	TBN*
17	Knowledge Transfer	5.2.3	TBN*

*TBN- To be negotiated

7.4 Instructions for deliverables

All the work products and deliverables should conform to the industry best practices such as Rational Unified Processes (RUP), Business Process Execution Language (BPEL) or equivalent methodology. Further, all work products and deliverables should be prepared using publicly available software such that FIU-IND can modify the work products and deliverables to meet changes in operating environment. Deliverables are to be delivered in accordance with the terms of the contract as well as any special instructions in the Work Requirements. For each deliverable, the Consultant shall provide a description of the deliverable contents. The deliverables/ work product should contain:

i) Reference number associated with the deliverable/ work product.

ii) Name of Deliverable/work product.

iii) Whether the document is a deliverable or a work product.

iv) The Date/ Milestone at which the deliverable/ work product will be provided to the FIU-IND.

v) Whether the deliverable/ work product is being originally created or updated.

vi) Any special notes or comments.

Documents and other products are to be delivered in accordance with the terms of the Work Requirements and in accordance with any additional instructions in the Work Requirements. Work products that are not deliverables shall remain under Consultant custody in a manner approved by the FIU-IND until the conclusion of the task, when they will be turned over to the FIU-IND. The Consultant shall document entire proceedings for the duration of the Consultancy project to establish information and document trail as well as help future analysis of any deficiencies in the project planning and management, if any, by following accepted best practices and also would help as a guide for continuous improvement.

8 INSTRUCTIONS TO THE CONSULTANT

8.1 Procedure for Submission of EoI

8.1.1 The Consultant should submit two hard copies of the Expression of Interest (EoI) and one soft copy in a sealed cover.

8.1.2 Each copy of EoI should be a complete document and should be bound as a volume separately. The document should be page numbered and appropriately flagged and contain the list of contents with page numbers. Different copies must be bound separately. The deficiency in documentation may result in the rejection of the Bid.

8.1.3 The soft copy of the EoI should be submitted, in the form of a non-re-writeable CD (Compact Disc). The CD media must be duly signed by the Consultant using a "Permanent Pen/Marker" and should bear the name of the Consultant.

8.1.4 The sealed cover should be super scribed with the wordings "Hiring of Consultant for the Project FINnet".

8.1.5 The sealed cover should also indicate clearly the name, address and telephone number of the Consultant to enable the proposal to be returned unopened in case it is declared "Late".

8.1.6 Consultant must ensure that the information furnished by him/her in respective CDs is identical to that submitted by him/her in the original paper document. In case of any discrepancy observed in the contents of the CDs and original paper documents, the information furnished on original paper document will prevail over the soft copy.

8.2 Cost of EoI

8.2.1 The Consultant shall bear all costs associated with the preparation and submission of its EOI, including cost of presentation for the purposes of clarification of the bid, if so desired by the Purchaser. FIU-IND will in no case be responsible or liable for those costs, regardless of the conduct or outcome of the Tendering process.

8.3 Contents of the EoI

8.3.1 The Consultant is expected to examine all instructions, forms, terms & conditions and Statement of Work in the EoI documents. Failure to furnish all information required or submission of an EoI Document not substantially responsive to the EoI in every respect will be at the Consultant's risk and may result in the rejection of the EoI.

8.4 Conflict of Interest

8.4.1 The Consultant who is selected for preparing the Consultancy Report will be barred from participating in the bidding process for its implementation. The Consultant and each of its subcontractors shall be disqualified from subsequently providing goods, works or services for such preparation or implementation.

8.5 Language of Bids

8.5.1 The Bids prepared by the Consultant and all correspondence and documents relating to the bids exchanged by the Consultant and the Purchaser, shall be written in the English language, provided that any printed literature furnished by the Consultant may be written in another language so long the same is accompanied by an English translation in which case, for purposes of interpretation of the bid, the English translation shall govern.

8.6 Confidentiality

8.6.1 FIU-IND requires that recipients of this document to maintain its contents in the same confidence as their own confidential information and refrain from any public disclosure whatsoever.

8.7 Disclaimer

8.7.1 FIU-IND and/or its officers, employees disclaim all liability from any loss or damage, whether foreseeable or not, suffered by any person acting on or refraining from acting because of any information including statements, information, forecasts, estimates or projections contained in this document or conduct ancillary to it whether or not the loss or damage arises in connection with any omission, negligence, default, lack of care or misrepresentation on the part of FIU-IND and/or any of its officers, employees.

8.8 Authorized Signatory (Consultant)

8.8.1 The "Consultant" as used in the EoI shall mean the one who has signed the EoI document forms. The Consultant should be the duly Authorized Representative of the Consultant, for which a certificate of authority will be submitted. All certificates and documents (including any clarifications sought and any subsequent correspondences) received hereby, shall, as far as possible, be furnished and signed by the Authorized Representative.

8.8.2 The power or authorization, or any other document consisting of adequate proof of the ability of the signatory to bind the Consultant shall be annexed to the bid. FIU-IND may reject outright any proposal not supported by adequate proof of the signatory's authority.

8.9 Subcontractor related conditions

8.9.1 The Consultant shall have the option to submit the proposal either alone or along with other subcontractors including the parent company/firm.

8.9.2 The Consultant shall be the sole point of contact for all purposes of the Contract. The Consultant will have the prime and sole responsibility for the execution of the Statement of Work.

8.9.3 In case of a EoI with subcontractors, the Consultant would need to submit a Memorandum of Understanding (MoU) / Agreement with the subcontractor clearly indicting their relationship. Such a MoU should be prepared on a stamp paper of requisite value. Proposals fulfilling partial requirements would be summarily rejected.

8.9.4 The subcontractors should not be involved in any major litigation that may have an impact of affecting or compromising the delivery of services as required under this contract. The Consultant or any of the subcontractors should not have been black-listed by any Central / State Government or Public Sector Undertakings. If at any stage of Tendering process or during the currency of the Contract, any suppression / falsification of such information is brought to the knowledge, FIU-IND shall have the right to reject the proposal or terminate the contract, as the case may be, without any compensation to the Tenderer.

8.10 Contact details of the Consultant

8.10.1 Consultant who want to receive FIU-IND's response to queries should give their contact details to FIU-IND. The Consultant should send their contact details in writing at the FIU-IND's contact address indicated in Para 1.2 of this document.

8.11 Queries on the EoI Document

8.11.1 Consultant requiring any clarification on this Document may send a query in writing at the FIU-IND's contact address indicated in Para 1.2 of this document. FIU-IND's response (including an explanation of the query but without identifying the source of inquiry) to all the queries, received not later than the dates prescribed by the FIU-IND in Para 1.2 of this document, will be made avaible on the website and sent to all Consultants who have given their contact details. FIU-IND may also hold a conference to give clarifications and invitation of the same will be sent to the Consultants who have given their contact details.

8.12 Amendment of EoI

8.12.1 At any time prior to the last date for receipt of bids, FIU-IND, may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective Consultant, modify the EoI Document by an

amendment. In order to provide prospective Consultants reasonable time in which to take the amendment into account in preparing their bids, FIU-IND may, at its discretion, extend the last date for the receipt of Bids and/or make other changes in the requirements set out in the Invitation for EOI.

8.13 Bid Processing Fees

8.13.1 All bids must be accompanied by a bid processing fee of INR 1,000 (INR One Thousand only) in the form of a crossed demand draft drawn on any nationalized/ scheduled bank payable at par in New Delhi, in favour of "The DDO, Financial Intelligence Unit-India, New Delhi". In case the document is downloaded from the website, bid processing fee of INR 1,500 would be required.

8.14 Documents Comprising the EOI

8.14.1 The proposal prepared by the Consultant shall comprise the following components:

i) EoI Form 1 : EoI Letter Proforma (refer Para 10.1)

ii) EoI Form 2 : Minimum Eligibility (refer Para 10.2)

iii) EoI Form 3 : Prior Experience (refer Para 10.3)

iv) EoI Form 4 : Comments and Suggestions (refer Para 10.4)

v) EoI Form 5 : Approach and Methodology (refer Para 10.5)

vi) EoI Form 6 : Declaration Letter (refer Para 10.6)

vii) Bid processing fee of INR 1,000 (INR One Thousand only) or INR1,500/-, as the case may be.

viii) Registered Power of Attorney executed by the Consultant in favor of the Principal Officer or the duly Authorized Representative, certifying him/her as an authorized signatory for the purpose of this EOI.

ix) Memorandum of Understanding (MoU) / Agreement prepared on a stamp paper of requisite value with the subcontractor clearly indicting their relationship. (In case of subcontractors)

8.14.2 FIU-IND shall not be responsible for non-receipt / non-delivery of the EoI due to any reason whatsoever. Consultants are advised to study the EoI document carefully. Submission of EoI shall be deemed to have been done after careful study and examination of the EoI document with full understanding of its implications.

9 SELECTION PROCESS

9.1 Pre-Qualification Criteria

The Consultant interested in being considered for this project must fulfill the following criteria:

i) Should be a firm/company registered/incorporated in India

ii) Should have at least 100 consultants on permanent pay roll in India as on March 31, 2006.

iii) Should have an minimum annual turnover of INR Two hundred million (INR 2,00,000,000) or its equivalent in foreign currency from Consulting Fees in each of the last three (3) years i.e. FY 2002-03, 2003-04 and 2004-05.

iv) Should have been profitable for at least two (2) of the last three (3) years i.e. FY 2002-03, 2003-04 and 2004-05.

v) Should have experience in

(i) Design of Anti Money Laundering/Risk Assessment Systems

(ii) Process Design

(iii) Information Systems Design

(iv) Information Security Planning

(v) Project Management

Experience of sub-contractor including parent company may be stated only if the relevant Memorandum of Understanding (MoU) is submitted.

vi) Should not be involved in any major litigation that may have an impact of affecting or compromising the delivery of services as required under this contract

vii) Should not be black-listed by any Central / State Government / Public Sector Undertaking in India

9.2 Preliminary Scrutiny

Preliminary scrutiny of the proposal will be made to determine whether they are complete, whether required process fee has been furnished, whether the documents have been properly signed, and whether the bids are generally in order. Proposals not conforming to such preliminary requirements will be prima facie rejected.

9.3 Evaluation of Proposals

The proposals would be evaluated on the basis of the pre-qualification criteria and Consultant's prior experience in the areas of Design of Anti Money Laundering/Risk Assessment Systems, Process Design, Information Systems Design, Information Security Planning and Project Management. The specific experience of the Consultant would be evaluated on the basis of the following information:

i) Evidence of having successfully carried out similar assignments.

ii) Evidence of having successfully carried out assignments with Government.

iii) Sufficient size, organization, and management to carry out the entire project.

iv) Specialized skills and access to particular technologies related to the assignment.

However, FIU-IND in its sole/absolute discretion can apply whatever criteria deemed appropriate in determining the responsiveness of the EoI submitted by the respondents. After evaluation, only those respondents who have been short-listed shall be duly informed in writing. The Request for Proposal / Tender Document shall be given to the short-listed respondents only.

10 EoI FORMS

EoI is to be submitted in the following format along with the necessary documents as listed. The EoI shall be liable for rejection in the absence of requisite supporting documents. EoI should provide information against each of the applicable requirements. In absence of the same, the EoI shall be liable for rejection.

10.1 EoI Form 1 : EoI Letter Proforma

To

The Director, FIU-IND
Financial Intelligence Unit-India
6th Floor, Hotel Samrat
Chanakyapuri, New Delhi -110021
India

Sir,

Sub: Hiring of Consultant for the Project FinNET

The undersigned Consultants, having read and examined in detail all the EoI documents in respect of appointment of a Consultant for Financial Intelligence Unit- India, do hereby express their interest to provide Consultancy Services as specified in the scope of work

2. Correspondence Details

Our correspondence details are:

1	Name of the Consultant	
2	Address of the Consultant	
3	Name of the contact person to whom all references shall be made regarding this tender	
4	Designation of the person to whom all references shall be made regarding this tender	
5	Address of the person to whom all references shall be made regarding this tender	
6	Telephone (with STD code)	
7	E-Mail of the contact person	
8	Fax No. (with STD code)	

3. Document forming part of EOI

We have enclosed the following:

i) EoI Form 2 : Minimum Eligibility (refer Para 10.2)

ii) EoI Form 3 : Prior Experience (refer Para 10.3)

iii) EoI Form 4 : Comments and Suggestions (refer Para 10.4)

iv) EoI Form 5 : Approach and Methodology (refer Para 10.5)

v) EoI Form 6 : Declaration Letter (refer Para 10.6)

vi) Bid processing fee

vii) Registered Power of Attorney executed by the Consultant in favor of the Principal Officer or the duly Authorized Representative, certifying him/her as an authorized signatory for the purpose of this EoI

viii) Memorandum of Understanding (MoU) / Agreement prepared on a stamp paper of requisite value with the subcontractor clearly indicting their relationship. (Optional)

4. We hereby declare that our EoI is made in good faith and the information contained is true and correct to the best of our knowledge and belief.

Thanking you,

Yours faithfully

(Signature of the Consultant)

Name :
Designation :
Seal :
Date :
Place :
Business Address:

Witness:		**Consultant:**	
Signature	_____	Signature	_____
Name	_____	Name	_____
Address	_____	Designation	_____
	_____	Company	_____
Date	_____	Date	_____

10.2 EoI Form 2 : Minimum Eligibility

[The Consultant should not include the figures of the subcontractors for EoI Form 2]

S.No.		FY 2002-03		
1.1	Name of Firm/Company			
1.2	Year of Registration/Incorporation			
1.3	Year of Registration/Incorporation in India*			
1.4	Number of Employees in India as on March 31, 2006			
		FY 2002-03	**FY 2003-04**	**FY 2004-05**
1.5	Annual Turnover from Consultancy Services**			
1.6	Annual Profits **			

*Enclose a copy of Registration document
**Enclose a copy of Audited Financial Statement with respect to information furnished in 1.5 and 1.6

Witness:
Signature _____
Name _____
Address _____
_____
Date _____

Consultant:
Signature _____
Name _____
Designation _____
Company _____
Date _____

10.3 EoI Form 3 : Prior Experience

[*Using the format below, provide information on each assignment for which your firm, and each associate for this assignment, was legally contracted either individually as a corporate entity or as one of the major companies within an association, for carrying out consulting services similar to the ones requested under this assignment. The Consultant should give information about maximum of five projects covering the areas of design of Anti Money Laundering/Risk Assessment Systems, Process Design, Information Systems Design, Information Security Planning and Project Management. Experience of sub-contractor including parent company may be stated only if the relevant Memorandum of Understanding (MoU) is submitted*]

Name of Consultant/Firm:	
Assignment/job name:	
Nature of Assignment:	*[Mention area(s) from the following:* - *Design of Anti Money Laundering/Risk Assessment System* - *Process Design* - *Information Systems Design* - *Information Security Planning* - *Project Management]*
Description of Project	
Approx. value of the contract (in Rupees):	
Country:	
Location within country:	
Duration of Assignment/job (months) :	
Name of Employer:	
Address and contact details:	
Total No of staff-months of the Assignment/job:	
Approx. value of the Assignment/job provided by your firm under the contract (in Rupees):	
Start date (month/year):	
Completion date (month/year):	
Name of associated Consultants, if any:	
No of professional staff-months provided by associated Consultants:	

Name of senior professional staff of your firm involved and functions performed.	
Description of actual Assignment/job provided by your staff within the Assignment/job:	

Note : Please attach Letter of Intent or Purchase Order or certificate of successful completion for each project, from the respective Client(s).

Witness:
Signature _____
Name _____
Address _____
_____
Date _____

Consultant:
Signature _____
Name _____
Designation _____
Company _____
Date _____

10.4 EoI Form 4 : Comments and Suggestions

[*Suggest and justify here any modifications or improvement to the scope of work, tasks to be performed, timeline, deliverables, payment terms etc. to improve performance in carrying out the Assignment. The Consultant can suggest deleting some activity or adding another, or proposing a different phasing of the activities. Such suggestions should be concise and to the point.*]

(Maximum two pages)

10.5 EoI Form 5 : Approach and Methodolgy

[Explain your understanding of the objectives of the Assignment/job, approach to the Assignment/job, methodology for carrying out the activities and obtaining the expected output, and the degree of detail of such output. You should highlight the problems being addressed and their importance, and explain the technical approach you would adopt to address them. You should also explain the methodologies you propose to adopt and highlight the compatibility of those methodologies with the proposed approach]
(Maximum two pages)

10.6 EoI Form 6 : Declaration Letter.

[*Declaration of sub-contractor including parent company is also needed if the relevant Memorandum of Understanding (MoU) is submitted*]

Declaration Letter on official letter head stating the following:

i) We are not involved in any major litigation that may have an impact of affecting or compromising the delivery of services as required under this contract

ii) We are not black-listed by any Central / State Government / Public Sector Undertaking in India

Witness:		**Consultant:**	
Signature	_____	Signature	_____
Name	_____	Name	_____
Address	_____	Designation	_____
	_____	Company	_____
Date	_____	Date	_____