Financial Management Federal Shared Service Provider Screening Criteria

INSTRUCTIONS: There are two sets of questions: one for previously designated Financial Management Line of Business (FMLoB) providers seeking to remain a provider and a second for federal agencies interested in becoming a Federal Shared Service Provider (FSSP) for financial management.

Choose the applicable section and answer the questions by checking "yes" or "no". Where requested, provide the applicable supporting reference materials or written explanations (100 words or less per question) in the form of an attachment (web links will not be reviewed).

A response of "no" to any of the screening criteria will automatically disqualify the Applicant from being selected as a FSSP.

Questions for previously designated FMLoB providers:

#	Information Requested	Response
Service Offerings and Technology Requirements		
1	Provides all of the mandatory financial management service offerings listed in *Supplemental Form A: Service Offerings* (definitions for the terms can be found in Appendix B)? To be considered to be a FSSP the Applicant must support both systems and transaction processing for the mandatory financial management service offerings.	■ Yes ☐ No
2	Is on the most current version of a supported financial system, or has an approved modernization plan that is currently being implemented?	■ Yes ☐ No
Capital Requirement		
3	Has a revolving fund (e.g., franchise or working capital fund) in place that currently is used for providing the financial management service offerings? Provide the legal citation for the fund with your submission.	■ Yes ☐ No
Compliance and Security Requirements		
4	Meets all current OMB and Department of Treasury requirements related to financial management listed below, or is scheduled to comply by the required deadline? Identify the status of those initiatives currently under development with your submission. More information on many of the initiatives can be found at http://www.fms.treas.gov/CFO_letter041113.pdf. • Provision of Treasury Accounting Symbol (TAS) / Business Event-Type Code (BETC) for all types of transaction, at time of transaction • Submission of Collections data in TAS/BETC format to Collections Information Repository (CIR) • Reporting to Central Accounting Reporting System (CARS) • Submission of payment data in standard format for Secure Payment System (SPS), Payment Automation Manager (PAM), International Treasury Services (ITS.gov), and the Automated Standard Application for Payments (ASAP) system • Implementation of the Do Not Pay standard business rules • Submission of bulk files to Government-wide Treasury Account Symbol Adjusted Trial Balance System (GTAS) • Submission of Intragovernmental Payment and Collections (IPAC) data in TAS/BETC format • Submission of payment data in TAS/BETC format to the Payment Information Repository (PIR) if a Non-Treasury Disbursing Office (NTDO) • Compliance with Federal Financial Management System Requirements (Treasury Financial Manual, Volume 1, Chapter 9500) • Compliance with Intragovernmental Business Rules (Treasury Financial Manual, Volume 1, Chapter 4700)	■ Yes ☐ No

#	Information Requested	Response
5	Provides a SSAE 16 Type II on all systems within the offering for its external customers or will provide one by September 30, 2014?	■ Yes ☐ No
6	Undergone a Federal Information Security Management Act (FISMA) review using NIST 800-53, Rev. 4, within the last 12 months without identification of significant deficiencies, or if significant deficiencies were identified they have been resolved or a plan is in place for them to be resolved? If applicable, describe the significant deficiencies and their resolution/plan for resolution.	■ Yes ☐ No
7	Received a Security Assessment and Authorization (SA&A), widely known as Risk Management Framework (RMF) Step 4 (Assess) and Step 5 (Authorize) as outlined within NIST SP 800-37, Rev. 1, on all systems within the offering within the last three years?	■ Yes ☐ No
8	Has a Continuity of Operations Plan (COOP) and successful Disaster Recovery Testing has been performed on all systems within the offering?	■ Yes ☐ No
9	Provides a formal Computer Security Incident Response Capability (CSIRC)? Provide the plan with the submission.	■ Yes ☐ No
10	Performs periodic testing and evaluation of information security controls? Summarize the type of testing and how often with your submission.	■ Yes ☐ No
11	Implemented a NIST SP 800-137 Continuous Monitoring Plan? Summarize the plan with your submission.	■ Yes ☐ No
12	Has an appointed information systems security officer (ISSO)? List their name, title and organization with your submission.	■ Yes ☐ No
13	Has coordinated contingency planning with the agency or agencies using its services? Provide the supporting artifact(s) with the submission (e.g., procedure).	■ Yes ☐ No
14	Has an interconnection security agreement and a Memorandum of Understanding (MOU) in accordance with NIST SP800-47?	■ Yes ☐ No
15	Does the data center proposed in the solution by the Applicant comply with all location and citizenship requirements of the agency?	■ Yes ☐ No

Questions for federal agencies interested in becoming a federal shared service provider for financial management:

#	Information Requested	Response
Service Offerings **and** Technology Requirements		
1	Provides all of the mandatory financial management service offerings listed in *Supplemental Form A: Service Offerings* (definitions for the terms can be found in Appendix B)? To be considered to be a FSSP the Applicant must support both systems and transaction processing for the mandatory financial management service offerings.	☐ Yes ☐ No
2	Is on the most current version of a supported financial system, or has an approved modernization plan that is currently being implemented?	☐ Yes ☐ No
Capital Requirement		
3	Has a revolving fund (e.g., franchise or working capital fund) in place that currently is, or can and will be, used for providing the financial management service offerings? Provide the legal citation for the fund with your submission.	☐ Yes ☐ No
Compliance and Security Requirements		
4	Meets all current OMB and Department of Treasury requirements related to financial management listed below, or is scheduled to comply by the required deadline? Identify the status of those initiatives currently under development with your submission. More information on many of the initiatives can be found at http://www.fms.treas.gov/CFO_letter041113.pdf. • Provision of Treasury Accounting Symbol (TAS) / Business Event-Type Code (BETC) for all types of transaction, at time of transaction	☐ Yes ☐ No

#	Information Requested	Response
	• Submission of Collections data in TAS/BETC format to Collections Information Repository (CIR) • Reporting to Central Accounting Reporting System (CARS) • Submission of payment data in standard format for Secure Payment System (SPS), Payment Automation Manager (PAM), International Treasury Services (ITS.gov), and the Automated Standard Application for Payments (ASAP) system • Implementation of the Do Not Pay standard business rules • Submission of bulk files to Government-wide Treasury Account Symbol Adjusted Trial Balance System (GTAS) • Submission of Intragovernmental Payment and Collections (IPAC) data in TAS/BETC format • Submission of payment data in TAS/BETC format to the Payment Information Repository (PIR) if a Non-Treasury Disbursing Office (NTDO) • Compliance with Federal Financial Management System Requirements (Treasury Financial Manual, Volume 1, Chapter 9500) • Compliance with Intragovernmental Business Rules (Treasury Financial Manual, Volume 1, Chapter 4700)	
5	Commits to providing a SSAE 16 Type II to its external customers by September 30, 2014?	☐ Yes ☐ No
6	Undergone a Federal Information Security Management Act (FISMA) review using NIST 800-53, Rev. 4, within the last 12 months without identification of significant deficiencies, or if significant deficiencies were identified they have been resolved or a plan is in place for them to be resolved? If applicable, describe the significant deficiencies and their resolution/plan for resolution.	☐ Yes ☐ No
7	Received a Security Assessment and Authorization (SA&A), widely known as Risk Management Framework (RMF) Step 4 (Assess) and Step 5 (Authorize) as outlined within NIST SP 800-37, Rev. 1, on all systems within the offering within the last three years?	☐ Yes ☐ No
8	Has a Continuity of Operations Plan (COOP) and successful Disaster Recovery Testing has been performed on all systems within the offering?	☐ Yes ☐ No
9	Provides a formal Computer Security Incident Response Capability (CSIRC)? Provide the plan with the submission.	☐ Yes ☐ No
10	Performs periodic testing and evaluation of information security controls? Summarize the type of testing and how often with your submission.	☐ Yes ☐ No
11	Implemented a NIST SP 800-137 Continuous Monitoring Plan? Summarize the plan with your submission.	☐ Yes ☐ No
12	Has an appointed information systems security officer (ISSO)? List their name, title and organization with your submission.	☐ Yes ☐ No
13	Commits to putting in place coordinated contingency planning with the agency or agencies using its services?	☐ Yes ☐ No
14	Commits to complete an interconnection security agreement and a Memorandum of Understanding (MOU) in accordance with NIST SP800-47 by September 30, 2104?	☐ Yes ☐ No
15	Does the data center proposed in the solution by the Applicant comply with all location and citizenship requirements of the agency?	☐ Yes ☐ No

Supplemental Form A: Mandatory Service Offerings

INSTRUCTIONS: In the table below, select the checkbox(s) next to each service offering that you provide and, where applicable, indicate whether it is offered in the form of systems support, transaction processing or both. Note that to be designated a FSSP for financial management an applicant must provide both systems support and transaction processing for all of the service offerings listed. Definitions for each service offering are provided in Appendix B: Financial Management Products & Services Catalog.

Grouping	Service Offering	Support Provided
Financial Management Services	Budget Execution	☐ System ☐ Transaction Processing
	General Ledger Accounting	☐ System ☐ Transaction Processing
	Financial Reporting	☐ System ☐ Transaction Processing
	Accounts Payable	☐ System ☐ Transaction Processing
	Accounts Receivable	☐ System ☐ Transaction Processing
	Intra-Governmental Accounting	☐ System ☐ Transaction Processing
	Grants Accounting	☐ System ☐ Transaction Processing
	Property Accounting	☐ System ☐ Transaction Processing
	Travel Accounting	☐ System ☐ Transaction Processing
	Cost Accounting	☐ System ☐ Transaction Processing
	Charge Card Accounting	☐ System ☐ Transaction Processing
	Audit Support	☐ System ☐ Transaction Processing
Technology Hosting and Administration	IT Hosting	☐ Yes ☐ No
	IT Administration Services	☐ Yes ☐ No
	IT Security Services	☐ Yes ☐ No
	Authorization and Accreditation	☐ Yes ☐ No
	Information System Security	☐ Yes ☐ No
	Customer Support Services	☐ Yes ☐ No
	Network Services	☐ Yes ☐ No
Application Management Services	Application Software Management	☐ Yes ☐ No
	Application Performance Management	☐ Yes ☐ No
	Continuity Planning	☐ Yes ☐ No
	Application Security Administration	☐ Yes ☐ No
	Application Software Development	☐ Yes ☐ No
	Application Data Management	☐ Yes ☐ No
	Interfaces Supported	☐ Yes ☐ No
System Implementation Services	Project Management Support	☐ Yes ☐ No
	Requirements Analysis	☐ Yes ☐ No
	Business Process Management	☐ Yes ☐ No
	System Migration Management	☐ Yes ☐ No
	System Conversions	☐ Yes ☐ No
	Testing	☐ Yes ☐ No
	Training Services	☐ Yes ☐ No
	Change Management	☐ Yes ☐ No

Financial Management Federal Shared Service Provider Screening Criteria Supplement

11-29-2013

Interior Business Center

LEGAL CITATION

RE #3 – Legal citation for working capital fund currently in place for providing financial management service offerings.

STATEMENT OF LEGAL AUTHORITY

The Interior Business Center (IBC), Office of the Secretary, Department of the Interior agrees to provide services and/or product support as outlined below, pursuant to authority under 43 U.S.C. §1467 and §1468, which established the DOI Working Capital Fund, and/or under the authority of Economy Act, 31 U.S.C. §1535. A detailed description of the services and/or product support is included as an attachment to the Inter-Agency Agreement.

OMB AND TREASURY REQUIREMENTS

RE #4 - Meets all current OMB and Department of Treasury requirements listed below that are related to financial management, or is scheduled to comply by the required deadline. Identify the status of those initiatives currently under development.

1. Provision of Treasury Accounting Symbol (TAS) / Business Event-Type Code (BETC) for all types of transaction, at time of transaction
   YES – IBC plans to meet the required deadline of January 2014.
2. Submission of Collections data in TAS/BETC format to Collections Information Repository (CIR)
   YES – IBC plans to meet the required deadline of January 2014.
3. Reporting to Central Accounting Reporting System (CARS)
   YES – This has already been met by the IBC
4. Submission of payment data in standard format for Secure Payment System (SPS), Payment Automation Manager (PAM), International Treasury Services (ITS.gov), and the Automated Standard Application for Payments (ASAP) System
   YES – IBC plans to meet all required deadlines of October 2014
   - **SPS – This has already been met by the IBC**
   - **ITS – This has already been met by the IBC**
5. Implementation of the Do Not Pay standard business rules
   YES – This has already been met by the IBC
6. Submission of bulk files to Government-wide Treasury Account Symbol Adjusted Trial Balance System (GTAS)
   YES – Plan to meet required deadline of December 2013 with reporting in Jan. 2014

7. Submission of Intra-governmental Payment and Collections (IPAC) data in TAS/BETC format

YES – This has already been met by the IBC

8. Submission of payment data in TAS/BETC format to the Payment Information Repository (PIR) if a Non-Treasury Disbursing Office (NTDO)

YES – IBC Plans to meet the required deadline of January 2014

9. Compliance with Federal Financial Management System Requirements (Treasury Financial Manual, Volume 1, Chapter 9500)

YES – This has already been met by the IBC

10. Compliance with Intra-governmental Business Rules (Treasury Financial Manual, Volume 1, Chapter 4700)

YES – This has already been met by the IBC

↗ FISMA REVIEW

RE #6 – Has undergone a Federal Information Security Management Act (FISMA) review using NIST 800-53, Rev. 4, within the last 12 months.

At the Department level, DOI has not yet migrated to Rev 4 and the IBC must follow their schedule. The upgrade of CSAM by DOI is pending; the planned implementation is for 2nd QTR FY15. All IBC systems have undergone a FISMA compliant A&A and as of FY14 were migrated to the Continuous Monitoring program. The IBC has consistently had a clean audit opinion utilizing the current model.

↗ COMPUTER SECURITY INCIDENT RESPONSE

RE #9 – Provide copy of CSIRC (computer security incident response capability).

The Interior Business Center does have a computer security incident response plan in place. The document supporting this is attached.

↗ SECURITY CONTROLS

RE #10 – Perform periodic testing and evaluation of information security controls. Summarize the type of testing and how often.

Each year the IBC undergoes a "Statements on Standards for Attestation Engagement" (SSAE-16) audit to examine the hosting and process of clients' transactions. During this engagement the controls are tested for the suitability of the design and their operating effectiveness related to the control objectives

stated in their descriptions. The General and Technology Controls of the Security Program that are tested are:

1. Logical Access
2. Physical Access
3. Change Control
4. Backup and Environmental Controls
5. Production Control

The Accounting Operations Controls that are tested are:

1. Input Controls
2. Processing Controls
3. Output Controls
4. Application Security

The IBC also conducts monthly vulnerability scans on our hosting and applications environments, and conducts quarterly scans of our databases and web portals. We have Intrusion Detection System (IDS) monitoring, and have Data Loss Prevention filtering that scans all outgoing email, file transfers, and web access for sensitive and personal identifiable information (PII).

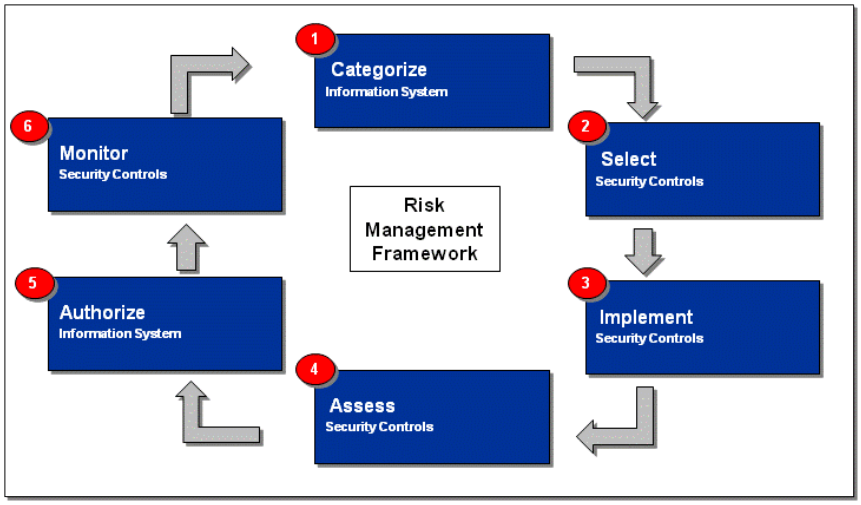
In addition we conduct internal A-123 reviews and testing on all our Accounting Operations to ensure compliance with OMB Circular A-123 - Management's Responsibility for Internal Control.

↗ CONTINUOUS MONITORING

RE #11 – Implemented a NIST SP 800-137 Continuous Monitoring Plan. Summary of the plan follows.

The IBC Continuous Monitoring Program implements automated monitoring, metrics, and reporting capabilities for all information domains identified by NIST. OMB has identified Configuration Management, Patch Management, and Vulnerability Management as the initial domains to monitor. Asset Management and Network Management have been recently added by IBC to augment the other three initial domains.

The Risk management Framework (RFM) promotes the concept of near real-time risk management and ongoing information system authorization through the implementation of robust continuous monitoring processes.



Step 1 - Categorize the information system and the information processed, stored, and transmitted by that system based on an impact analysis.

Step 2 - Select an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions.

Step 3 - Implement the security controls and describe how the controls are employed within the information system and its environment of operation.
Step 4 - Assess the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Step 5 - Authorize information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.
Step 6 - Monitor the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.
The following tools and methodologies are utilized to measure security control effectiveness on a continuous basis:

1. **Asset Management.** The practice of managing the entire life cycle (design, construction, commissioning, operating, maintaining, repairing, modifying, replacing and decommissioning/disposal) of physical and infrastructure assets such as servers, desktop, and laptops.
2. **Intrusion Detection System (IDS).** Signature -based inspection of network traffic to detect intrusions and has the ability to perform real-time traffic analysis and packet logging on networks.
3. **Data Loss Prevention (DLP).** DLP is a comprehensive (network layer / endpoint) solution; a content-aware solution that discovers, monitors, and protects confidential data / PII wherever it is stored or transmitted – across network, storage and endpoint systems.
4. **Security Information and Event Management (SIEM).** SIEM is for centralized collection and correlation of system and network events.
5. **Change Advisory Board Meetings**. Used to enforce change management.
6. **Vulnerability Management**. Vulnerability management scans are used to determine weaknesses in the environment.
7. **Network Access Control (NAC).** NAC is a networking solution that implements policies that control access to networks when devices initially attempt to access the network.
8. **CyberScope.** The Department of Homeland Security in conjunction with the Department of Justice is developing an application, CyberScope, to handle manual and automated inputs of agency data for FISMA reporting.

Endpoint Protection. Endpoint is the concept that each device (end point) is responsible for its own security. Firewall, virus / malware scanners and other intrusion detection or intrusion prevention application are responsible for securing an end-point.

↗ INFORMATION SYSTEMS SECURITY

RE #12 – Name and title of information systems security officer (ISSO).

At the IBC each system has an ISSO that reports to the System Owner. The system owner reports to Chief, Quality Assurance Section because he/she has Application Security Oversight for the IBC Financial Management Directorate. In turn, the Quality Assurance Section Chief reports to the Chief Information Security Officer (CISO).

- Jeanette Dickman, Information Technology Specialist and OFF Operational Lead
  ISSO for Oracle Federal Financials
  Finance and Procurement Systems Division
  Interior Business Center, Financial Management Directorate
- Stacey Richkun
  Chief Information Security Officer (CISO)
  OCIO, Department of the Interior
- Julie Rundgren
  Chief, Quality Assurance Section
  Finance and Procurement Systems Division
  Interior Business Center, Financial Management Directorate

↗ CONTINGENCY PLANNING

RE #13 – Coordinated contingency plan with the agencies using services. Provide supporting artifact.

The Interior Business Center does have a contingency plan in place with our hosting facility and our customer agencies which is tested annually. The document supporting this is attached.