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 <u>mandatory</u> 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 <u>mandatory</u> 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

ESC FM SSP Screening Criteria Questions Supplemental Responses

3. (Q) 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, ESC currently operates in a Franchise Fund environment. The legal citation is attached per your request.

4. (Q) 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

  - Expected Implementation Aug 2014

- Submission of Collections data in TAS/BETC format to Collections Information Repository (CIR)

  - Expected Implementation Aug 2014

- Reporting to Central Accounting Reporting System (CARS) - Expected Implementation Aug 2014

- 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

  - Expected Implementation Aug 2014

- Implementation of the Do Not Pay standard business rules

  – Testing with Do Not Pay.

- Submission of bulk files to Government-wide Treasury Account Symbol Adjusted Trial Balance System (GTAS)

  – Expected Implementation 1/9/2014

- Submission of Intragovernmental Payment and Collections (IPAC) data in TAS/BETC format

  – Implemented Manually

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

- Not Applicable to ESC

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

  – Periodically reviewed to ensure compliance with Federal Financial Management goals

- Compliance with Intragovenrnmental Business Rules (Treasury Financial Manual, Volume 1, Chapter 4700)

  - We are in full compliance with the Intragovernmental Business Rules

6. (Q) 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, Delphi system personnel plan to have a NIST 800-53, Rev 4 assessment within FY14. Security documents are currently being created to comply with NIST 800-53, Rev 4, dated April 2013. The last FISMA review conducted in May 2013 was accomplished utilizing NIST 800-53, Rev. 3. POA&Ms are given for the discrepancies found after every assessment, audit, continuous monitoring activity, and security impact analysis. The Information System Security Officer (ISSO) will determine how long it will take to complete the finding and meet the minimum requirements of 800-53. Furthermore, the ISSO will be required to close out the POA&M at a defined time. Delphi POA&Ms statuses are reviewed at least every month for managerial purposes.

9. (Q) Provides a formal Computer Security Incident Response Capability (CSIRC)? Provide the plan with the submission.

Yes, however, Delphi utilizes Cyber Security Management Center (CSMC) for formal Security Incident Response Capability.

10. (Q) Performs periodic testing and evaluation of information security controls? Summarize the type of testing and how often with your submission.

Yes, Delphi follows the FAA Order 1370.82A (Page 3-2, section, 5a and b) and the DOT Cybersecurity Compendium, to perform system certification activities. Security controls for this system are assessed at least annually 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. A security assessment plan was developed and used which identifies the scope of the assessment, including the security controls/enhancements under assessment, assessment procedures, and assessment environment, including the assessment team roles and responsibilities. A security assessment report (SAR) was produced which documents the assessment results; and the results, as documented in the SAR were provided to the AO.

11. (Q) Implemented a NIST SP 800-137 Continuous Monitoring Plan? Summarize the plan with your submission.

Yes, Delphi is in a constant continuous monitoring stage as POA&M's are issued after the yearly SA package and routed to the Authorizing Official for signatures that permits the system to remain in operating status. The Security Operations Section conducts monthly spot checks for self-assessments of the eighteen Security Control Families. Delphi change control board and ISSOs track, monitor, and route changes through the appropriate personnel to accomplish a system change request. The ISSOs evaluate the security impact changes before alteration of the production environment. All changes to the system are outlined in the Delphi Configuration Management Plan (CMP) and ESC Prism Configuration Management Plan (CMP).

12. (Q) Has an appointed information systems security officer (ISSO)? List their name, title and organization with your submission.

Yes, two Information System Security Officers have been appointed.

> Primary ISSO
> Information System Security Organization, MMAC, OKC OK
> Delphi Alternate ISSO
> Information System Security Organization, MMAC, OKC OK

13. (Q) Has coordinated contingency planning with the agency or agencies using its services? Provide the supporting artifact(s) with the submission (e.g., procedure).

Yes, Delphi coordinates with Delphi customers for contingency tests and exercises. Organizational elements and key personnel are documented within the ISCP. The ISCP is tested twice a year.

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