

Supplement 10

TECHNICAL REQUIREMENT MATRIX

Instructions for Completing the Technical Requirements Self-Scoring Worksheet

1. The Contractor must self-score each MITS Technical Requirement in the "Response Code" column using only the values that appear in the drop-down list.

2. The "Response Code" values are:

- D** – Available as delivered without configuration, extension, or modification
- P** – Partially available as delivered without configuration, extension, or modification
- C** – Available with configuration
- M** – Requires a modification
- N** – Not available/Not met

3. Each requirement must contain one of the scoring values identified in Item #2 above. Any requirement without a scoring value will be considered to be "Not Met" ("N").

4. Comments **must** be included in the required narrative section of the Contractor's RFP reponse and the applicable narrative reference page number **must** be inserted in the Page Reference ("Page Ref") column for all requirements that are coded "P" (Requirement will be partially met with the delivered software without configuration, code extensions, or modification). These narrative comments must explain how the requirement will be partially met and which areas will not be met.

Instructions for Completing the Proposed Technologies Self-Scoring Worksheet

1. For each Technology Solution area, the Contractor must briefly identify (no more than 20 words) the proposed technology solution.

2. The Contractor must self-score each proposed technology in the "Preferred, Supported, or Other" column using only the values that appear in the drop down list. The drop-down list values are:

- P** - Preferred solution
- S** - Supported solution
- O** - Other solution

3. Each proposed technology solution must contain one of the scoring values identified in Item #2. Any technology solution without a scoring value will be considered non-compliant and no score will be calculated.

4. Comments **must** be included the required narrative section of the Contractor's RFP response and the applicable narrative reference page number **must** be inserted in the Page Reference ("Page Ref") column for each Technology Solution coded as "O" (Other). These narrative comments must explain the proposed techology and the standards and/or best practices that will be employed with the technology.

MITS Technical Requirement "Fit" Survey				
Requirement Number	Requirement	Phase (1 or 2)	Response Code	Page Ref
1.0	General Application Architecture			
1.1	Use Open Standards			
1.1.1	Use open data and technical standards that align with MITA & FEA;			
1.1.2	Use/ leverage commercial off the shelf systems (COTS) or components as far as possible;			
1.2	Use Component / Layered Based Architecture			
1.2.1	Solution must be based on an n-tier component based application architecture;			
1.2.2	Solution must be built using component based frameworks;			
1.3	Server Operating Systems			
1.3.1	Solution may run on a UNIX based operating system (e.g. AIX, Solaris) or Windows based OS with the exception of the database servers;			
1.4	Other			
1.4.1	An overriding requirement is for all components of the solution to have a current significant market share.			
2.0	Access Channels (User Interfaces)			
2.1	MITS user interface used must take advantage of the Internet standards because of the diverse nature of users across the state.			
2.2	MITS must use Web browsers, no client component download. Prefer a thin client, browser agnostic solution; if client downloaded components are required for any user category, they must be identified with supplemented with business and technical justifications.			
2.3	MITS must not use any proprietary web browsers.			
2.4	Use standard document sharing tool : Adobe PDF for document sharing.			
2.5	MITS user interface must be compliant with American Disabilities Act (ADA) guidelines.			
2.6	The access channel must be fully integrated with the security requirements.			
3.0	Data Sharing and Interoperability (Integration)			

Select only codes from the drop-down lists to complete this survey.

Requirement Number	Requirement	Phase (1 or 2)	Response Code	Page Ref
3.1	MIT S must use industry standard communication mechanisms such as HL7, X12 (EDI), XML, LOINC.			
3.2	All shared data must be made available through standardized interfaces with the capability to provide transparent access to data from their sources.			
3.3	MIT S must use industry standard integration tools.			
3.4	All communications must be HIPAA compliant.			
4.0	Architecture Utility Services			
4.1	It is preferred that MIT S have a process automation and workflow service component that will simplify the automation of process that span the MIT S Medicaid enterprise. It will also simplify maintenance of process changes in the future.			
4.2	MIT S must use a rules engine that is easy to maintain and change. This will facilitate the ongoing maintenance of the business rules in the future.			
4.3	MIT S must have an imaging component that integrates with content management and process automation areas.			
5.0	Data Management and Reporting			
5.1	Data Management			
5.1.1	The vendor must propose industry standard data conversion tools and strategy to facilitate data conversion.			
5.1.2	MIT S must have a batch data import and export tool or have a strategy to achieve easy import and export of data as needed.			
5.1.3	MIT S must allow for replication of database master structure and data that can be used for ad hoc reports and queries.			
5.1.4	MIT S must facilitate communication with data warehouses and provide analysis capability within the solution.			
5.2	Reporting			

Requirement Number	Requirement	Phase (1 or 2)	Response Code	Page Ref
5.2.1	MITS must support Ad hoc reporting, operation reports and canned reports.			
5.2.2	Ad hoc reporting must be presented via user friendly interface and preferably in a commercially available tool.			
5.2.3	Reports must be run against non-transactional data store.			
5.3	Database			
5.3.1	MITS database must to be a Relational Database Management System (i.e. DB2, Oracle).			
5.3.2	Provide a documented data model, data dictionary and data meta model of the underlying database structure and logic electronically.			
6.0	Security and Privacy			
6.1	Infrastructure			
6.1.1	MITS must be able to support the firewalls and intrusion detection system that is maintained by DAS.			
6.1.2	MITS must employ a layered approach to protecting data.			
6.1.3	It is preferred that MITS use products from multiple vendors to mitigate the risk of any one vendor's product being compromised.			
6.1.4	The solution preferably should logically separate the database and SAN devices from the remainder of the centralized application architecture by keeping it on a separate network.			
6.1.5	The architecture should be configured so that no external source (except administrators) can directly access the database. The only access to the database is via the business layer which enforces business rules and validates all data to keep the database clean and protected.			
6.2	Authentication, Authorization and Administration			
6.2.1	Security must be role based, both at the user and group level. The roles must be tied to the business areas within Medicaid enterprise.			

Requirement Number	Requirement	Phase (1 or 2)	Response Code	Page Ref
6.2.2	Access roles must be able to be defined at the individual data element.			
6.2.3	<p>MITS must use granular role-based security that can limit the functionality for an individual or groups of individuals. This includes controlling access to individual screens and fields. Screens and fields should be able to be hidden entirely, or presented in read-only mode, preventing any updates by unauthorized users.</p> <p>Temporary workers should be assigned security rights that allow them access to only the specific functions required for their jobs.</p>			
6.2.4	MITS must provide integrated security for the application and the database.			
6.2.5	MITS must utilize the primary security tool (Identity Management System) for access control. Security needs to be LDAP based (Novell eDirectory).			
6.2.6	MITS must follow State guidelines for the restriction of override capabilities of the Identity Management System.			
6.2.7	The security system must utilize the Identity Management System for security protocols and access.			
6.2.8	The Identity Management System must support online, real-time updating of security information.			
6.2.9	MITS must be able to provide ad-hoc reporting capabilities on state-defined security metrics.			
6.2.10	Passwords must expire on a periodic basis and be reset at any time by appropriate personnel and/or automated system reset.			
6.2.11	MITS must log and report all unauthorized access attempts by source IP (if available), user ID, date, and time.			
6.2.12	MITS must automatically remove individual security profile upon notification of termination, but save profile for archival purposes, with the functionality to re-use the profile if needed.			

Requirement Number	Requirement	Phase (1 or 2)	Response Code	Page Ref
6.2.13	MITS must automatically disable access to any user after a predetermined number of attempts to log-on.			
6.2.14	MITS must have the ability to log a user off the system if there is no activity within a configurable period of time.			
6.2.15	MITS must have the ability to terminate access if there is no activity on a user account within a configurable period of time.			
6.2.16	MITS must be designed to support data encryption such as the use of SSL for data transmission.			
7.0	Support and Administration			
7.1	Availability			
7.1.1	MITS must be available for access at a minimum during ODJFS core working hours (are 6:00 a.m. to 7:00 p.m., Eastern Standard Time, Monday through Friday, and on Saturdays 8:00 a.m. to 12:00 p.m., Eastern Standard Time, except for State observed holidays, and on an emergency basis if requested by the State).			
7.1.2	Data base system is available and accessible to multiple users 24X7 except for ODJFS-approved time for system maintenance.			
7.1.3	The Medicaid Portal, and other system components as required by ODJFS, must be available 7 days a week, 24 hours a day, except agreed upon downtime.			
7.2	Performance and Scalability			
7.2.1	MITS must be able to be scaled incrementally as use grows.			
7.2.2	Vendor must provide a package upgrade strategy that preserves solution customizations.			
7.2.3	Vendor must provide hardware benchmarks in order to properly size the hardware requirements for MITS prior to implementation in each of the environments.			

Requirement Number	Requirement	Phase (1 or 2)	Response Code	Page Ref
7.2.4	MITs must have a strategy to support capacity growth.			
7.2.5	MITs must provide performance tuning mechanisms.			
7.3	Backup and Disaster Recovery			
7.3.1	MITs implementation must have a robust backup procedure.			
7.3.2	Vendor must provide a documented Disaster Recovery plan and restart procedures.			
7.3.3	Vendor must provide a Configuration Management Plan.			
7.4	Other			
7.4.1	MITs must integrate with existing OIT/ODJFS system monitoring tools.			
8.0	System Documentation			
8.1	Requirement Documents			
8.1.1	Requirements management plan			
8.1.2	Change management plan			
8.2	Design Documents			
8.2.1	Process Model Diagrams			
8.2.2	System Design Specifications			
8.2.3	Logical and Physical Data Model			
8.2.4	Data Dictionary			
8.2.5	Technical Architecture			
8.2.6	Capacity Plan			
8.2.7	Network Architecture Diagram /Schematics /Guide			
8.2.8	Hardware configuration Diagram /Schematics /Guide			
8.3	Implementation and Support documents			
8.3.1	Operations Manual			
8.3.2	Desktop Guide			
8.3.3	Training Plan			
8.3.4	Training Guide			
8.3.5	Security Plan			
8.3.6	Implementation Plan			
8.3.7	Post Implementation Support plan			
8.3.8	Disaster Recovery Plan			
8.3.9	Back Up Plan			

Requirement Number	Requirement	Phase (1 or 2)	Response Code	Page Ref
8.3.10	Transition & Staffing plan			
8.3.11	Configuration Management Plan			
8.3.12	Conversion Pplan			
8.4	Other			
8.4.1	MITS must have context sensitive help			

MITS Proposed Technologies Survey

System Platform

Technology Summary			
	Server Hardware Platform(s)	Desktop Hardware Platform(s)	Operating System(s)
The preferred solution is:	IBM Power RISC Sun Sparc RISC	X86(Intel/AMD)	AIX(Server)* Solaris(Server)* *latest GA versions
ODJFS currently supports:	IBM Power RISC Sun Sparc RISC X86(Intel/AMD) based systems	X86(Intel/AMD)	AIX (Server 5L - v5.2.x, v5.3.x) Solaris(Server v9, v10) Linux (Server) HP-UX Windows XP Windows Server 2003 (Enterprise, Data Center Edition) HP OpenView
Proposed Solution Assessment			
	Proposed Solution	Preferred, Supported, or Other	Page Reference
Server Hardware Platform (s)			
Desktop Hardware Platform (s)			
Operation System (s)			

Web Client

Technology Summary			
	External User Interface – Thin Client	Internal User Interface	Component Architecture
The preferred solution is:	Web Browser Hypertext Markup	Web Browser HTML	J2EE 1.4 standard
ODJFS currently supports	Language (HTML) Web Browser (IE v6.x or higher, Netscape v4.x or higher)	Rich Client	N-Tier J2EE 1.3, 1.4 .NET, N-tier, client-server
Proposed Solution Assessment			
	Proposed Solution	Preferred, Supported, or Other	Page Reference
External User Interface – Thin Client			
Internal User Interface			
Component Architecture			

Web, Application and Portal server software

Technology Summary			
	Web Server(s)	Application Server(s)	Portal Server(s)
The preferred solution is:	HTTP	WebSphere Application Server (Network Deployment) and related components	WebSphere Portal Server
ODJFS currently supports	IBM HTTP 2.0.x, 6.0.x on AIX, Solaris Microsoft IIS on x86(Intel/AMD) Apache on Unix	WebSphere Application Server v5.1.x, v6.0.x on AIX, Solaris, Linux - .NET Framework (Windows 2003 Server Data Center Edition) -Microsoft BizTalk Server 2004	IBM Websphere Portal Extend v5.1.x on AIX, Solaris, Linux -Microsoft Commerce Server -Microsoft SharePoint Portal
Proposed Solution Assessment			
	Proposed Solution	Preferred, Supported, or Other	Page Reference
Web Server(s)			
Application Server(s)			
Portal Server(s)			

MITS Proposed Technologies Survey				
Data Management and Reporting				
Technology Summary				
	Data Management	Reporting	RDBMS	Job Scheduler
The preferred solution is:	Informatica	Cognos ReportNet	Oracle on Unix DB2 UDB on Unix	BMC Control-M BMC EM
ODJFS currently supports	Informatica DB2 Load Utilities SQL Loader IDCAMS File Aid	Cognos Series7 Cognos ReportNet Crystal Enterprise	DB2 UDB Oracle 9i, 10g (RAC, Data Guard) MS SQL Server	BMC Control-M BMC EM
Proposed Solution Assessment				
	Proposed Solution	Preferred, Supported, or Other	Page Reference	
Data Management				
Reporting				
RDBMS				
Job Scheduler				

Security			
Technology Summary			
	Identity Management/ Single Sign On	Authentication	Business Rules Engine
The preferred solution is:	Novell eDirectory, Tivoli Identity Manager, Tivoli Access Manager, Tivoli WebSeal	Novell eDirectory	
ODJFS currently supports	Novell eDirectory 8.7.x Tivoli Identity Manager v4.6.x, Tivoli Access Manager 5.1.x, Tivoli WebSeal	Novell eDirectory 8.7.3 Microsoft Active Directory	ILog JRules
Proposed Solution Assessment			
	Proposed Solution	Preferred, Supported, or Other	Page Reference
Identity Management/ Single Sign On			
Authentication			
Business Rules Engine			

MITS Proposed Technologies Survey			
Network/System/Application Monitoring			
Technology Summary			
	Network Monitoring/Intrusion Detection/Event Management	Performance Monitoring	Transaction/ Application /Resource Monitoring
The preferred solution is:	Tivoli Enterprise - Console/NetView Compuware Vantage Nagios(open source) DAS provided IDS service	Tivoli Omegamon XE Oracle Enterprise Manager WebTrends	Tivoli Omegamon XE Tivoli TMTP InsightETE
ODJFS currently supports	Nagios HP Openview Compuware Vantage Tivoli Enterprise Console/NetView DAS provided IDS service	Tivoli Omegamon XE (Distributed, WAS, WBI, Database, MQ, MQSI)- Oracle Enterprise Manager WebTrends	Tivoli Omegamon XE InsightETE, Tivoli TMTP
Proposed Solution Assessment			
	Proposed Solution	Preferred, Supported, or Other	Page Reference
Network Monitoring/Intrusion Detection/Event Management			
Performance Monitoring			
Transaction/ Application /Resource Monitoring			

MITS Proposed Technologies Survey			
Imaging/Process Workflow			
Technology Summary			
	Electronic Document Management	Workflow Management /Messaging	
The preferred solution is:	FileNet P8 Content Manager FileNet P8 BPM FileNet Records Manager FileNet eForms FileNet Image Manager FileNet Federation Services KoFax Ascent Capture Suite	FileNet P8 BPM	
ODJFS currently supports	FileNet P8 BPM FileNet eForms Adobe eForms FileNet P8 Content Manager FileNet Records Manager FileNet Image Manager FileNet Federation services KoFax Ascent Capture Suite v6.x	Websphere Business Integration Server v4.3 (Workflow, Interchange, Message Broker) Websphere Business Integration Modeler and Monitor v5.1.x FileNet P8 BPM (Mandatory) MSMQ Microsoft Message Queuing	
Proposed Solution Assessment			
	Proposed Solution	Preferred, Supported, or Other	Page Reference
Electronic Document Management			
Workflow Management /Messaging			

MITS Proposed Technologies Survey			
Call Center/Help Desk			
Technology Summary			
	Call Center	CRM	Email/Messaging/ Secure Email
The preferred solution is:	MITS must interface with the current (or scaled up) Rockwell/Concerto ACD based Integrated Call Center IVR/VRU/ACD/PBX infrastrucure (Nortel Succession PBX,		SMTP (application server) Novell Groupwise Interface with ODJFS managed Secure Email system
ODJFS currently supports	SBC managed infratructure Nortel Succession PBX Rockwell ACD		SMTP (application servers) Novell Groupwise IBM MessagePlus/Open
Proposed Solution Assessment			
	Proposed Solution	Preferred, Supported, or Other	Page Reference
Call Center			
CRM			
Email/Messaging/Secure Email			

Support Tools				
Technology Summary				
Domain	ODJFS Software	Proposed Solution	Preferred, Supported, or Other	Page Reference
Service Management (Help Desk) System	BMC Remedy			
Configuration/Change Management	Merant Dimensions, IBM Rational ClearQuest, PVCS SCLM			
Business Process Modeling/Collaboration	IBM Websphere BI Modeler v5.1.x, Websphere BI Monitor			
Database Modeler	ERWIN/Allfusion Data Modeler IBM Rational Rose Data modeler			
Document Management/Collaboration	Documentum eRoom v7.x			
Project Management	MS-Project			
Requirements & Analysis	IBM Rational Requisite Pro MS-Visio			
Application Design & Construction	IBM Rational Team Unifying Platform v6.xx IBM Rational Rose XDE Dev for Java IBM Rational Software Modeler			
Application Testing Suite	Mercury QuickTest Pro Mercury LoadRunner Mercury Test Director			
Forms/Notice creation	Adode - Forms Server, Designer, Reader Extension, Central Pro, Output Designer, Web Output, Barcode Output Forms Metavante - CSF Designer			
ZIP+4 software	Pitney Bowes Finalist(Mainframe), Centrus AddressBroker			
AFP to PDF conversion	TargetStream StreamA2P			
Secure File Transfer	Sterling Commerce Connect:Direct			

MITS Proposed Technologies Survey				
Web Content Management	Serena Collage			
Data Management & Migration	Informatica			

Supplement 11

Declaration Regarding Material Assistance / Nonassistance to a Terrorist Organization



GOVERNMENT BUSINESS AND FUNDING CONTRACTS
In accordance with section 2909.33 of the Ohio Revised Code

DECLARATION REGARDING MATERIAL ASSISTANCE/NONASSISTANCE TO A TERRORIST ORGANIZATION

This form serves as a declaration of the provision of material assistance to a terrorist organization or organization that supports terrorism as identified by the U.S. Department of State Terrorist Exclusion List (see the Ohio Homeland Security Division website for a reference copy of the Terrorist Exclusion List).

Any answer of "yes" to any question, or the failure to answer "no" to any question on this declaration shall serve as a disclosure that material assistance to an organization identified on the U.S. Department of State Terrorist Exclusion List has been provided. Failure to disclose the provision of material assistance to such an organization or knowingly making false statements regarding material assistance to such an organization is a felony of the fifth degree.

For the purposes of this declaration, "material support or resources" means currency, payment instruments, other financial securities, funds, transfer of funds, and financial services that are in excess of one hundred dollars, as well as communications, lodging, training, safe houses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel, transportation, and other physical assets, except medicine or religious materials.

Form with fields: LAST NAME, FIRST NAME, MIDDLE INITIAL, HOME ADDRESS, CITY, STATE, ZIP, COUNTY, HOME PHONE, WORK PHONE.

COMPLETE THIS SECTION ONLY IF YOU ARE A COMPANY, BUSINESS OR ORGANIZATION

Form with fields: BUSINESS/ORGANIZATION NAME, BUSINESS ADDRESS, CITY, STATE, ZIP, COUNTY, PHONE NUMBER.

DECLARATION

In accordance with division (A)(2)(b) of section 2909.32 of the Ohio Revised Code

For each question, indicate either "yes," or "no" in the space provided. Responses must be truthful to the best of your knowledge.

- 1. Are you a member of an organization on the U.S. Department of State Terrorist Exclusion List?
2. Have you used any position of prominence you have with any country to persuade others to support an organization on the U.S. Department of State Terrorist Exclusion List?

GOVERNMENT BUSINESS AND FUNDING CONTRACTS - CONTINUED

3. Have you knowingly solicited funds or other things of value for an organization on the U.S. Department of State Terrorist Exclusion List?
 Yes No
4. Have you solicited any individual for membership in an organization on the U.S. Department of State Terrorist Exclusion List?
 Yes No
5. Have you committed an act that you know, or reasonably should have known, affords "material support or resources" to an organization on the U.S. Department of State Terrorist Exclusion List?
 Yes No
6. Have you hired or compensated a person you knew to be a member of an organization on the U.S. Department of State Terrorist Exclusion List, or a person you knew to be engaged in planning, assisting, or carrying out an act of terrorism?
 Yes No

In the event of a denial of a government contract or government funding due to a positive indication that material assistance has been provided to a terrorist organization, or an organization that supports terrorism as identified by the U.S. Department of State Terrorist Exclusion List, a review of the denial may be requested. The request must be sent to the Ohio Department of Public Safety's Division of Homeland Security. The request forms and instructions for filing can be found on the Ohio Homeland Security Division website.

CERTIFICATION

I hereby certify that the answers I have made to all of the questions on this declaration are true to the best of my knowledge. I understand that if this declaration is not completed in its entirety, it will not be processed and I will be automatically disqualified. I understand that I am responsible for the correctness of this declaration. I understand that failure to disclose the provision of material assistance to an organization identified on the U.S. Department of State Terrorist Exclusion List, or knowingly making false statements regarding material assistance to such an organization is a felony of the fifth degree. I understand that any answer of "yes" to any question, or the failure to answer "no" to any question on this declaration shall serve as a disclosure that material assistance to an organization identified on the U.S. Department of State Terrorist Exclusion List has been provided by myself or my organization. If I am signing this on behalf of a company, business or organization, I hereby acknowledge that I have the authority to make this certification on behalf of the company, business or organization referenced on page 1 of this declaration.

X

Signature

Date

Supplement 12

Excluded Entities List

Ohio Department of Public Safety
Ohio Homeland Security

U.S. Department of State Terrorist Exclusion List

Terrorist Exclusion List Designees

- Al-Ittihad al-Islami (AIAI)
- Al-Wafa al-Igatha al-Islamia
- Asbat al-Ansar
- Darkazanli Company
- Salafist Group for Call and Combat (GSPC)
- Islamic Army of Aden
- Libyan Islamic Fighting Group
- Makhtab al-Khidmat
- Al-Hamati Sweets Bakeries
- Al-Nur Honey Center
- Al-Rashid Trust
- Al-Shifa Honey Press for Industry and Commerce
- Jaysh-e-Mohammed
- Jamiat al-Ta'awun al-Islamiyya
- Alex Boncayao Brigade (ABB)
- Army for the Liberation of Rwanda (ALIR) -- AKA: Interahamwe, Former Armed Forces (EX-FAR)
- First of October Antifascist Resistance Group (GRAPO) -- AKA: Grupo de Resistencia Anti-Fascista Premero De Octubre
- Lashkar-e-Tayyiba (LT) -- AKA: Army of the Righteous
- Continuity Irish Republican Army (CIRA) – AKA: Continuity Army Council
- Orange Volunteers (OV)
- Red Hand Defenders (RHD)
- New People's Army (NPA)
- People Against Gangsterism and Drugs (PAGAD)
- Revolutionary United Front (RUF)
- Al-Ma'unah
- Jayshullah
- Black Star
- Anarchist Faction for Overthrow
- Red Brigades-Combatant Communist Party (BR-PCC)
- Revolutionary Proletarian Nucleus
- Turkish Hizballah
- Jerusalem Warriors
- Islamic Renewal and Reform Organization
- The Pentagon Gang
- Japanese Red Army (JRA)
- Jamiat ul-Mujahideen (JUM)
- Harakat ul Jihad i Islami (HUJI)
- The Allied Democratic Forces (ADF)
- The Lord's Resistance Army (LRA)

Ohio Department of Public Safety
Ohio Homeland Security

Designated on February 18, 2003

- Al Taqwa Trade, Property and Industry Company Ltd. (f.k.a. Al Taqwa Trade, Property and Industry; f.k.a. Al Taqwa Trade, Property and Industry Establishment; f.k.a. Himmat Establishment)
- Bank Al Taqwa Ltd. (a.k.a. Al Taqwa Bank; a.k.a. Bank Al Taqwa)
- Nada Management Organization (f.k.a. Al Taqwa Management Organization SA)
- Youssef M. Nada & Co. Gesellschaft M.B.H.
- Ummah Tameer E-Nau (UTN) (a.k.a. Foundation for Construction; a.k.a. Nation Building; a.k.a. Reconstruction Foundation; a.k.a. Reconstruction of the Islamic Community; a.k.a. Reconstruction of the Muslim Ummah; a.k.a. Ummah Tameer I-Nau; a.k.a. Ummah Tamir E-Nau; a.k.a. Ummah Tamir I-Nau; a.k.a. Ummat Tamir E-Nau; a.k.a. Ummat Tamir-I-Pau)
- Loyalist Volunteer Force (LVF)
- Ulster Defense Association (a.k.a. Ulster Freedom Fighters)
- Afghan Support Committee (a.k.a. Ahya ul Turas; a.k.a. Jamiat Ayat-ur-Rhas al Islamia; a.k.a. Jamiat Ihya ul Turath al Islamia; a.k.a. Lajnat el Masa Eidayul Afghania)
- Revival of Islamic Heritage Society (Pakistan and Afghanistan offices -- Kuwait office not designated) (a.k.a. Jamia Ihya ul Turath; a.k.a. Jamiat Ihia Al- Turath Al-Islamiya; a.k.a. Revival of Islamic Society Heritage on the African Continent)

SUPPLEMENTAL INFORMATION TRAILER

This page is the last page of supplemental information for this competitive document. If you received this trailer page, all supplemental information has been received.

Note: portions of the supplemental information provided may or may not contain page numbers. The total number of pages indicated on the cover page does not include the pages contained in this supplement.