Appendix C - Functional Requirements Definition/Detailed Design Compliance Matrix

This section provides a compliance matrix documenting and ensuring that the unique requirements identified in the Government Electronic Directory Functional Requirements Document (FRD) are met in the Detailed Design. The matrix contains the unique FRD identifier, a description of the requirement, the section in the FRD in which the requirement is specified, and the section in the Detailed Design Document in which the requirement is satisfied through a design specification.

NUMBER	DESCRIPTION	FRD SECTION	DESIGN SECTION
	GENERAL REQUIREMENTS		
G1	The Government Electronic Directory must implement the protocols, services, and functions defined in the 1993, and later, versions of the ITU-T X.500 series of recommendations.	2.1	1.3.1 2.1.1
G2	The Government Electronic Directory must provide an electronic White Page service to its users.	2.1.1.1	1.5.5
G3	The Government White Pages must provide the capability to restrict Directory search and browse functions to a subset of the White Pages.	2.1.1.1	1.5.5
G4	The Government Directory must provide an electronic Blue Pages service to its users.	2.1.1.2	1.5.6
G5	The Government Electronic Directory must provide an electronic Yellow Pages service to its users.	2.1.1.3	1.5.8
G6	The Government Directory must provide an electronic Green Page service to its users.	2.1.1.4	1.5.7
G7	The Government Electronic Directory must support public users.	2.1.1.5	2.2.2
G8	The Government Electronic Directory must have the capability to support group lists for messaging and multicasting networks.	2.1.1.5	5.4
G9	The Government Electronic Directory must have the capability to support applications other than messaging that may be used by its users, such as Electronic Commerce/Electronic Data Interchange (EC/EDI) and work flow applications.	2.1.1.6	1.5.1 1.5.2 1.5.3
G10	The Government Electronic Directory must have the capability to support Public Key Cryptography.	2.1.1.6	1.5.3 4.1.2
G11	The Government Electronic Directory must be protected against physical threats (such as intruders, fire, and flood) and electronic and technical failures.	2.1.2.1	4.5.3 Agency Specific Design
G12	The Government Electronic Directory should provide the capability to verify the integrity of information sent and received.	2.1.2.1	Agency Specific Design

NUMBER	DESCRIPTION	FRD SECTION	DESIGN SECTION
	GENERAL REQUIREMENTS		
G13	The Government Electronic Directory must provide directory information needed to establish government communications.	2.1.2.1	2.1.11.4
G14	The Government Electronic Directory must, as appropriate, return the requested information it holds with a probability of greater than 99.99 percent.	2.1.2.1	Agency Specific Design
G15	The Government Directory should be available 24 hours a day, 7 days a week.	2.1.2.2	Agency Specific Design
G16	The Government Electronic Directory must support public access.	2.1.2.2	2.2.2
G17	Access to the Government Electronic Directory must be controlled.	2.1.2.2	4.4
G18	Each agency must determine who is permitted to use the Government Electronic Directory and under what circumstances.	2.1.2.2	4.4.3
G19	The Government Electronic Directory must be designed to support multiple applications, drawn from a wide variety of possibilities, when technically feasible.	2.1.2.2	1.5.1
G20	The Government Directory must support both traveling and mobile users.	2.1.2.2	2.2.2
G21	The Government Electronic Directory must support full data replication and automatic data updating capabilities.	2.1.2.2	2.1.7
G22	The Government Electronic Directory must support the addition of components (hardware and software), such as Directory servers, as the network expands to support more government users.	2.1.2.3	2.1.11.3
G23	The Government Electronic Directory shall use International Standards Organization (ISO) protocols and TCP/IP.	2.1.2.3	2.2.2.2 2.2.3
G24	The Government Electronic Directory shall expand to a distributed architecture.	2.1.2.3	2.1.11.3
G25	If the Government Electronic Directory cannot deliver the information requested by a user, the user must be promptly notified of non-response from the Directory.	2.1.2.4	1.3
G26	The Government Electronic Directory must unambiguously verify that the information marked as originating from a given source within the Government Electronic Directory domain did, in fact, originate there.	2.1.2.4	4.3
G27	The Government Electronic Directory must provide accountability and audit trail for all queries and support the analysis of both security monitoring and security-related events (e.g., successful/unsuccessful log-on attempts, violations of security procedures/policies).	2.1.2.4	4.5.2

NUMBER	DESCRIPTION	FRD SECTION	DESIGN SECTION
	GENERAL REQUIREMENTS		
G28	The Government Electronic Directory must allow authorized users to access information wherever it may be maintained in the Government Electronic Directory domain.	2.1.2.6	4.4.1 4.4.3
G29	The Government Electronic Directory should be able to integrate the legacy directories used in Federal, State, Local and Tribal Governments.	2.1.2.6	2.1.11.3
G30	The Government Electronic Directory must support interfaces to X.500 directory systems outside the Government Electronic Directory domain.	2.1.2.6	2.1.11.4
G31	Government Directory components (hardware and software) must be backward compatible with previous versions of ITU-T X.500 (1988) series of recommendations.	2.1.2.6	1.3 2.1.1
G32	Testing must be employed to ensure Government Directory components and services function together in an interoperable manner.	2.1.2.6	To Be Determined
G33	To ensure uniqueness of naming information on a Government basis, common naming and registration procedures shall be used.	2.1.2.6	3.0
G34	The E-Mail PMO should establish, administer, and enforce the set of rules (i.e., schema) governing the Directory Information Base.	2.1.2.6	3.1
G35	The Government Electronic Directory components should be deployed over a wide variety of transport networks, including those that use OSI, TCP/IP, and LAN protocols.	2.1.2.6	2.2.3.2
G36	The Government Electronic Directory must be able to support commercial and government authentication mechanisms.	2.1.2.6	4.1
G37	The Government Electronic Directory must use Universal Time Coordinated (UTC) as the standard for time reference.	2.1.2.6	Not Applicable
G38	The Government Electronic Directory should have the capability to dynamically adjust to changing network loads and conditions, where technically and economically feasible, to provide timely delivery of Directory information.	2.1.2.7	Agency Specific Design
G39	The Government Directory must provide near real-time response to queries.	2.1.2.7	Agency Specific Design
G40	On command, the Government Directory must allow its users to discontinue any search.	2.1.2.7	2.1.3
G41	The information contained in the Government Electronic Directory must be capable of replication to improve performance.	2.1.2.7	2.1.7

NUMBER	DESCRIPTION	FRD SECTION	DESIGN SECTION
	GENERAL REQUIREMENTS		
G42	The Government Electronic Directory should provide a standard interface to allow agencies to participate in the Government Electronic Directory through directory synchronization techniques.	2.1.2.7	2.1.11.4
G43	The Government Electronic Directory must have the ability to cache data.	2.1.2.7	2.1.7
G44	The Government Electronic Directory users must be able to address a message quickly and easily.	2.1.2.7	Agency Specific Design
G45	The Government Electronic Directory must recognize and process queries based on precedence.	2.1.2.7	Agency Specific Design
G46	The probability of undetected query loss must be less than one query out of 100 million.	2.1.2.7	Agency Specific Design
G47	Access to the Government Electronic Directory must be intuitive and predictable to individuals and organizations.	2.1.2.8	2.2
G48	The Government Electronic Directory must have the capability of storing a variety of information describing all aspects of communications (e.g. phone, fax, E-Mail, postal address), as well as government information, such as personnel information (e.g. title, job description, salary, employment history).	2.1.2.8	5.0
G49	It must be easy for network administrators to add and modify data stored in the Government Electronic Directory.	2.1.2.8	2.2.3.3
G50	The Government Electronic Directory must support the use of aliases.	2.1.2.8	3.2.2 5.0
G51	Addresses in the Government Electronic Directory must be current and accurate.	2.1.2.9	Agency Specific Design
G52	Directory entries must be spell checked when created and updated.	2.1.2.9	Agency Specific Design
G53	Information objects must be registered in the Government Directory to ensure uniqueness and unambiguous identification of objects on a global basis.	2.1.3.1	5.0
G54	GSA must be the registration authority for the registration of newly identified and required object classes and attributes.	2.1.3.1	3.1
G55	User registration must be supported by registration authorities established in the user domain.	2.1.3.1	3.1.3
G56	The Government Directory must support on-line user registration, when necessary.	2.1.3.1	Agency Specific Design

NUMBER	DESCRIPTION	FRD SECTION	DESIGN SECTION
	GENERAL REQUIREMENTS		
G57	Government Electronic Directory systems administrators must use authentication procedures to obtain administrative access to the Directory.	2.1.3.3	2.2.3.3
G58	System Administrators must have access to a minimum set of Government Electronic Directory administration features.	2.1.3.3	2.2.3.3
G59	The Government Electronic Directory must be managed through a hierarchical management structure.	2.1.4	3.1
G60	The Government Electronic Directory must be based on the principles of interoperability, leading the Government's migration to international standards and protocols.	2.1.4.1	1.3 2.1.1
G61	All Government Electronic Directory software and hardware must be implemented in accordance with applicable government and/or government-approved standards.	2.1.4.1	5.0
G62	The Government Electronic Directory must allow for minimum required syntax changes to accommodate differences in capabilities between directory components and systems.	2.1.4.1	2.1.11.3
G63	An audit trail of the information to support performance monitoring must be provided by the Government Electronic Directory.	2.1.4.2	4.5.2
G64	An audit trail of the information to support fault isolation must be provided by the Government Electronic Directory.	2.1.4.3	4.5.2
G65	The Government Electronic Directory must incorporate appropriate self-test and diagnostic features, as well as supporting maintenance documentation.	2.1.4.3	4.5.2
G66	The Government Directory must support usage-sensitive billing.	2.1.4.4	To Be Determined
G67	The Government Electronic Directory must provide access control and security mechanisms to the attribute level.	2.1.4.5	4.4.1
G68	The Government Electronic Directory must generate and maintain audits of all security violations for 30 days.	2.1.4.5	4.5.2
G69	The Government Electronic Directory must comply with the Computer Security Act of 1987 (Public Law 100-235).	2.1.4.5	4.5.1
G70	No single hardware, software, and/or human error malfunction must allow security checks to be bypassed.	2.1.4.5	4.5.1
G71	The Government Electronic Directory must provide for the appropriate security measures, such as physical, personnel, INFOSEC, COMSEC, and COMPUSEC, in accordance with agency security policy.	2.1.4.5	4.5.1

NUMBER	GENERAL REQUIREMENTS	FRD SECTION	DESIGN SECTION

	DIRECTORY SYSTEM AGENT		
DSA1	The DSA must accept associations and binds from any authorized DUA, including DUAs integrated with other components.	2.2.1	2.2
DSA2	The DSA must support the Directory Access Protocol (DAP) as specified in the ITU-T X.500 specifications.	2.2.1	2.2.1
DSA3	The DSA must support Lightweight Directory Access Protocol (LDAP) as specified in RFC 1487.	2.2.1	2.2.1
DSA4	The DSA must support World Wide Web (WWW) to X.500 gateway functions.	2.2.1.1	2.2.1
DSA5	The DSA must support ANSI/NISO Z39.50 Wide Area Information Services (WAIS) to X.500 synchronization functions.	2.2.1.1	2.2.1
DSA6	The DSA must be able to store double-byte character sets to support international, non-English character strings.	2.2.1.1	Agency Specific Design
DSA7	The DSA must support interrogation and modification operations.	2.2.1.1	1.3
DSA8	The DSA must provide support for interactive user browsing.	2.2.1.1	2.1.2
DSA9	The DSA must support interfaces to other types of directories.	2.2.1.1	2.1.11.4
DSA10	The DSA must provide the capability to search and retrieve information based on any attribute or combination of attributes.	2.2.1.1	1.3
DSA11	The DSA must process queries by priority on a FIFO basis.	2.2.1.1	1.3
DSA12	The DSA must provide the capability to perform pre-programmed updates to entries (to allow for support of contingency operations) that become effective at a specified “effective time.” This should include one-step changeover of entire branches of the DIT.	2.2.1.1	Agency Specific Design
DSA13	The DSA must provide the capability for batch submission of Directory updates that eliminate the need for a continuous DUA-to-DSA bind for the DSA to process the request.	2.2.1.1	Agency Specific Design
DSA14	The DSA must provide the capability to apply a time stamp to each entry to indicate when the data were last modified and became effective.	2.2.1.1	1.3
DSA15	The DSA must provide the capability to receive requests for information from a DUA and hold information for the DUA until the user reestablishes the DUA-to-DSA bind and retrieves the information.	2.2.1.1	Agency Specific Design
DSA16	The DSA must allow fuzzy searches.	2.2.1.1	1.3
DSA17	The DSA must provide the capability to perform updates of naming information in non-leaf entries.	2.2.1.1	1.3
DSA18	The DSA must provide the capability for relocation and deletion of subtrees.	2.2.1.1	1.3
DSA19	The DSA must provide the capability to define new object classes or subclasses. New object classes may be defined as abstract, structural, or auxiliary.	2.2.1.1	1.3

NUMBER	GENERAL REQUIREMENTS	FRD SECTION	DESIGN SECTION
	DIRECTORY SYSTEM AGENT		
DSA20	The DSA must respond to interrogation and modification operations.	2.2.1.2	1.3
DSA21	The DSA must support Directory Operational Binding Management Protocol (DOP) as described in the ITU-T X.500 specifications.	2.2.2	1.3
DSA22	The DSA must support Directory Information Shadowing Protocol (DISP) as described in the ITU-T X.500 specifications.	2.2.2	2.1.3
DSA23	The DSA must permit and optionally inhibit the replication (shadowing) of information between DSAs.	2.2.2	2.1.3
DSA24	The DSA must support total and/or incremental strategies for updating shadowed information.	2.2.2	1.3
DSA25	The DSA must provide for the caching information retrieved as authorized by the local manager.	2.2.2.1	1.3
DSA26	Information cached by a Government DSA must be managed.	2.2.2.1	1.3
DSA27	The DSA must support and optionally inhibit Referral, Unichaining, and Multichaining operations with other DSAs.	2.2.2.2	2.1.10
DSA28	The schema must extend to all levels of implementation of the Government Electronic Directory.	2.2.3	1.3
DSA29	The DSA must support all standard object classes and attributes as defined in X.402. X.509, X.520, and X.521.	2.2.3	5.0
DSA30	The DSA must support the use of hierarchical attributes that allow attribute sets such that the group has a generic type that can be used to retrieve the entire group. The generic type, such as telephone number, could be used as a filter to return any of the subtypes, such as fax, mobile, and pager numbers.	2.2.3	5.0
DSA31	The DSA must support the 1993 extensions to the ITU-T X.500 Directory Services series of recommendations, such as collective attributes and operational attributes.	2.2.3	5.0
DSA32	The DSA must support the creation of object classes and attributes specifically for Government Directory use.	2.2.3	5.0
DSA33	Bulk loading of data from a non-X.500 database to X.500 must be supported.	2.2.3.1	1.3
DSA34	Directory synchronization for E-Mail addresses (e.g., SMTP and X.400) to and from X.500 must be supported.	2.2.3.1	5.0
DSA35	The Government Electronic Directory must provide the capability for the Distribution List functionality.	2.2.3.2	5.0
DSA36	The Government Electronic Directory must provide support of alias entries.	2.2.3.3	5.0
DSA37	The Government Electronic Directory is required to support the security requirements for protecting and safeguarding information that it contains and provides to Government components and users.	2.2.4	4.4

NUMBER	GENERAL REQUIREMENTS	FRD SECTION	DESIGN SECTION
	DIRECTORY SYSTEM AGENT		
DSA38	Information exchanged between any components of the Government Electronic Directory must be protected at the appropriate level.	2.2.4	4.3 4.4
DSA39	The DSA must support the 1993 ITU-T X.500 Directory Services Security model and the schemas defined for Basic Access Control and Simplified Access Control that are part of the standard (X.501).	2.2.4.1	4.4
DSA40	The DSA must be capable of simple or strong authentication of Directory components on every Directory access, as appropriate.	2.2.4.1	4.1
DSA41	Cryptographic security mechanisms should be used to provide strong authentication between DSAs and other components, when determined necessary.	2.2.4.1	4.1
DSA42	The DSA must provide for the capability to control access to Directory entries and attributes.	2.2.4.2	4.4
DSA43	The DSA must allow access control to be applied to entries, attributes, or attribute values by individuals or groups of individuals.	2.2.4.2	4.4
DSA44	The DSA must allow the owner of information in its DIB to restrict search actions.	2.2.4.2	4.5
DSA45	The DSA must be able to provide data integrity services and safeguards against accidental, unauthorized, or malicious actions that result in the alteration of Directory information.	2.2.4.2	4.4
DSA46	The DSA must provide the capability to use DSS digital signatures and algorithms to verify the integrity of requests and responses contained in DAP and DSP transmissions from DUAs and other DSAs, as defined by security policy when necessary.	2.2.4.2	4.3
DSA47	Confidentiality services must be provided to protect Directory queries, responses, and information transfers, when necessary, as defined by security policy.	2.2.4.2	4.3
DSA48	The DSA must provide safeguards against accidental, unauthorized, or malicious actions that result in the alteration of security protection mechanisms or access levels.	2.2.4.2	4.5.1 4.5.3
DSA49	The Government Directory requires sufficient capacity to contain entries for all Government users, provide interfaces to application entities and network resources, and meet Government response time goals.	2.2.5	2.1.6
DSA50	The Directory must provide adequate throughput to satisfy inquiries demanded by all its applications.	2.2.5	Agency Specific Design
DSA51	The DSA must support distribution of the DIB such that the response time for individual and cooperative lookups, updates, and replication updates is acceptable.	2.2.5	Agency Specific Design

NUMBER	GENERAL REQUIREMENTS	FRD SECTION	DESIGN SECTION
	DIRECTORY SYSTEM AGENT		
DSA52	The DSA must provide a response within 1 second from its collocated DIB.	2.2.5	Agency Specific Design
DSA53	The DSA must be able to support a deferred result service.	2.2.5	2.1.10
DSA54	The DSA availability must exceed 98.5 percent to support the writer-to-reader system availability for messages.	2.2.5	Agency Specific Design
DSA55	The DSA must support ITU-T X.700 management agents.	2.2.6	Agency Specific Design
DSA56	The DSA must support the production of event reports as defined in X.500.	2.2.6	1.3
DSA57	The DSA is required to produce management summary reports.	2.2.6	4.5.1
DSA58	The DSA must support system planning functions required to meet service-level agreements.	2.2.6	Agency Specific Design
DSA59	The DSA must support the transparent collection and reporting of Directory performance data.	2.2.6.2	4.5.1
DSA60	The DSA must provide fault management capabilities to detect and resolve problems internal to the DSA itself.	2.2.6.3	4.5.1
DSA61	The DSA must have the capability to collect and maintain proper accounting of Directory transactions and resource usage to support billing administration.	2.2.6.4	4.5.1
DSA62	Security management is required to ensure the integrity, protection, and validity of information contained in the DSAs.	2.2.6.5	4.5.1
DSA63	Security management functions must be supported by an auditing capability.	2.2.6.5	4.5.1
DSA64	The DSA is required to create and maintain audit logs of accesses to objects it protects.	2.2.6.5	4.5.1
DSA65	The DSA is required to permit audit data to be selectively acquired based on needs and policies of the Government.	2.2.6.5	4.5.1
DSA66	DSAs must interface with DUAs integrated with applications responsible for key management. DSAs and DUAs must support insertion and maintenance of certificate information in the Directory.	2.2.6.5	4.2
DSA67	Security documentation is required for review and conformance of the DSA.	2.2.6.5	4.5.1

NUMBER	DESCRIPTION	FRD SECTION	DESIGN SECTION
	DIRECTORY USER AGENT		

NUMBER	DESCRIPTION	FRD SECTION	DESIGN SECTION
	DIRECTORY USER AGENT		
DUA1	The DUA must provide users with the capability to use Directory information in interactions with other applications.	2.3.1	1.5.1 5.0
DUA2	The DUA must be flexible enough to support the display of new or non-standard attributes specified in the Government Directory schema.	2.3.1	2.2
DUA3	The DUA must have the capability to support user browsing, searches, and modification requests.	2.3.1	2.2
DUA4	The DUA must have the capability to allow a user to interactively browse through Directory information.	2.3.1	2.2
DUA5	At startup, the DUA must provide the capability to bind automatically to a previously specified DSA and, in the case of a bind failure, to an alternative DSA.	2.3.1	Agency Specific Design
DUA6	The DUA must provide a context sensitive “Help” capability.	2.3.1	2.2
DUA7	The DUA must provide the capability to assist users with the preparation of Directory queries.	2.3.1	2.2
DUA8	The DUA must support hyperlinking similar to the Internet standard Hyper-Text Markup Language (HTML).	2.3.1	2.2
DUA9	The Directory must provide users the capability to enter Directory information.	2.3.1	2.2
DUA10	The DUA must provide the capability to create non-standard schema elements.	2.3.1	5.0
DUA11	The DUA must provide the capability to create and modify Directory entries in batches.	2.3.1	Agency Specific Design
DUA12	The DUA must provide the capability to allow Directory modifications at preprogrammed times.	2.3.1	Agency Specific Design
DUA13	The DUA must provide a standard Application Programming Interface (API).	2.3.1	2.2.4
DUA14	The DUA must provide the capability to interact with a user in different languages or with different abilities.	2.3.1	Agency Specific Design
DUA15	The DUA must support the capability to perform an integrity check on request parameters before submitting requests to the Directory.	2.3.2	4.5.1
DUA16	The DUA must be able to submit a deferred results query to a DSA.	2.3.2	2.1.10
DUA17	The DUA must provide to a user or application all information requested.	2.3.3.1	Agency Specific Design
DUA18	The DUA must interpret an error response from a DSA and present an easy-to-understand error message to a user.	2.3.3.2	2.1.3

NUMBER	DESCRIPTION	FRD SECTION	DESIGN SECTION
	DIRECTORY USER AGENT		
DUA19	The DUA must provide the capability to reissue the query to the new DSA based on a referral from the previous DSA.	2.3.3.3	2.1.6
DUA20	The DUA must return the address information of the new DSA to the user if the DUA is not configured to reissue a referral.	2.3.3.3	2.1.10
DUA21	The DUA must provide the capability to locally cache information about recently or frequently queried objects and attributes.	2.3.4	Agency Specific Design
DUA22	The DUA must provide the capability for the user to select and store entries and attributes in a local directory.	2.3.4	Agency Specific Design
DUA23	The DUA must provide the capability to authenticate users.	2.3.5.1	4.1.1 4.1.2
DUA24	A DUA must provide the capability to authenticate itself to a DSA before binding.	2.3.5.1	4.1
DUA25	The DUA must provide the capability to support selective control of access to Directory information by authorized users.	2.3.5.2	4.4.1
DUA26	The DUA must provide the capability to protect the integrity of data transmitted to and received from the DSA.	2.3.5.3	4.3
DUA27	The DUA must provide the capability to support data confidentiality services.	2.3.5.4	4.3
DUA28	The DUA must provide the capability to generate audit trail logs of DUA activities.	2.3.5.5	4.5.2
DUA29	The DUA must ensure against disabling or bypassing of audit capabilities within the software.	2.3.5.5	4.5.2
DUA30	DUA availability must be at least 98.5 percent.	2.3.6	Agency Specific Design
DUA31	The DUA must provide the capability to support management agents that support Government Electronic Directory administrative and security functions.	2.3.7	4.5
DUA32	The DUA must provide the capability to support configuration management of the Directory.	2.3.7.1	2.2.3.3
DUA33	The DUA must support the capability to manage the DUA cache locally.	2.3.7.1	Agency Specific Design
DUA34	The DUA must be capable of generating and submitting its status and performance information to the management agent.	2.3.7.2	4.5.2
DUA35	The DUA must be capable of generating and submitting its fault management information to the management agent.	2.3.7.3	4.5.2

NUMBER	DESCRIPTION	FRD SECTION	DESIGN SECTION
	DIRECTORY USER AGENT		
DUA36	The DUA will provide the necessary information to support billing for Directory usage.	2.3.7.4	Agency Specific Design
DUA37	The DUA must preclude unauthorized access to its configuration data.	2.3.7.5	4.5.1
DUA38	Installation of a DUA in a component cannot preclude any of the requirements for managing security information in that component.	2.3.7.5	Agency Specific Design