ATTACHMENT K - ARDHS - OIT Standard IT Requirements

Requirement Number	Requirement Group	Requirement Subgroup	Requirement
1	Application Hosting	Batch – Job Control and Scheduling	Any technology vendor, application or solution shall develop, document and manage the processes and procedures for Interfaces and Batch Operations Architecture.
2	Application Hosting	Batch – Job Control and Scheduling	Any technology vendor, application or solution shall define job scheduling requirements, application software interdependencies, and rerun requirements for all production jobs
3	Application Hosting	Batch – Job Control and Scheduling	Any technology vendor, application or solution shall utilize and manage scheduling tools for automating job execution (e.g., job workflow processes interdependencies, rerun requirements, file exchange functions, and print management)
4	Application Hosting	Batch – Job Control and Scheduling	Any technology vendor, application or solution shall maintain a master job schedule and execute all batch jobs for the DHS Enterprise Program (e.g. any jobs provided by any vendor working on/with the DHS Enterprise Platform)
5	Application Hosting	Batch – Job Control and Scheduling	Any technology vendor, application or solution shall perform job monitoring and manage resolution of any failed jobs.
6	Application Hosting	Change/Release Management	Any technology vendor, application or solution shall adhere to the Information Technology Infrastructure Library (ITIL) V3.0 Change and Release Management processes.
7	Application Hosting	Change/Release Management	Any technology vendor, application or solution shall identify and submit any changes in compliance with the DHS Enterprise Program Change/Release Management process.
8	Application Hosting	Disaster Recovery	Any technology vendor, application or solution shall maintain a detailed Disaster Recovery plan to meet Disaster Recovery requirements. Plan shall include plans for data, back-ups, storage management, and contingency operations that provides for recovering the DHS Enterprise Platform within established recovery requirement timeframes after a disaster that has affected the users of the DHS Enterprise Platform.
9	Application Hosting	Disaster Recovery	Any technology vendor, application or solution shall provide support to the DHS support teams with implementing, configuring and testing disaster recovery.
10	Application Hosting	Disaster Recovery	Any technology vendor, application or solution shall develop action plans to address any issues arising from Disaster Recovery testing.
11	Application Hosting	Infrastructure Security	Any technology vendor, application or solution using cloud technology shall be located within the continental US. All servers and data will be located in US Soil.
12	Application Hosting	Infrastructure Security	Any technology vendor, application or solution shall proactively monitor all infrastructure including but not limited to network, storage, virtual environments, servers, databases, firewalls, etc. following industry best practices.
13	Application Hosting	Infrastructure Security	Any technology vendor, application or solution shall implement physical and logical security within new functionality defined in the security plan consistent with DHS' security policies and industry standards.
14	Application Hosting	Infrastructure Security	Any technology vendor, application or solution shall review all available infrastructure security patches relevant to the environment and classify the need and speed in which the security patches should be installed as defined by DHS security policies.
15	Application Hosting	Network, Hosting and Data Center Services	Any technology vendor, application or solution shall provision new environments and capacity as required to ensure performance requirements are met as volume increases and additional functionality is implemented.
16	Application Hosting	Operating System, Application and Database Backup and Recovery	Any technology vendor, application or solution shall encrypt all data at rest including backups using DHS and regulatory bodies (CMS, FNS, etc.) standards regardless of storage media.
17	Application Hosting	Storage Management Services	Any technology vendor, application or solution will provide data backup and restoration services in accordance with industry best practices.
18	Application Hosting	Storage Management Services	Any technology vendor, application or solution will recommend techniques and procedures to ensure disk storage resources are utilized in an efficient and cost-effective manner.
19	Application Hosting	Storage Management Services	Any technology vendor, application or solution shall regularly test recovery procedures and practices to demonstrate recoverability and verify that actual practices are in concert with procedures and report results, as well as meet business requirements
20	Application Hosting	Storage Management Services	Any technology vendor, application or solution shall monitor and demonstrate compliance with Arkansas Records Retention Schedule.

21	Application Hosting	System Monitoring	Any technology vendor, application or solution shall manage and maintain monitoring procedures and standards for system/solution/infrastructure including, but not limited to: a. Monitoring of buffers, database buffers, table space fragmentation, database space, for unusual growth and propose a solution in case of alert b. Monitoring of system logs, update error, database corruption, jobs execution failures etc. and propose solution in case of an alert c. Monitoring of alert notification interface (e.g., Simple Mail Transfer Protocol (SMTP), sendmail), and propose a solution in case of an alert d. Monitoring of transaction and trace logs, network event logs and traces, garbage collector, memory and CPU utilization, indexes, etc., and propose a solution in case of an alert e. Monitoring of middleware (e.g., workflows, in- and out-bound queues) and report to DHS according to agreed procedure f. Monitoring and reporting of end-to-end transaction response time to allow measurements against SLAs g. Monitoring of interfaces h. Monitoring of batch jobs and job scheduling
22	Application Hosting	System Monitoring	Any technology vendor, application or solution shall monitor infrastructure for availability as well as transaction and response time performance.
23	Application Hosting	System Monitoring	Any technology vendor, application or solution shall provide regular monitoring reports of infrastructure performance, utilization and efficiency (e.g., proactive system monitoring)
24	Application M&O Services	Disaster Recovery	Any technology vendor, application or solution shall identify and make available appropriate resources to support DHS' disaster recovery planning, testing and execution.
25	Application M&O Services	Security Administration	Any technology vendor, application or solution shall provide documented procedures for security monitoring and log management functions, and use write-once technology or other secure approaches for storing audit trails and security logs.
26	Data Governance	Master Data Management	Any technology vendor, application or solution shall provide data dictionary, data models, data flow models, process models and other related planning and design documents to DHS.
27	General System Behavior	Audit_&_Compliance	Any technology vendor, application or solution shall maintain a record (e.g. audit trail) of all additions, changes and deletions made to data in the applicable system or solution. In addition, a log of query or view access to certain type of records and/or screens will be maintained for investigative purposes. This should be readily searchable by user ID or client ID. This must include, but is not limited to: a. The user ID of the person who made the change b. The date and time of the change c. The physical, software/hardware and network location (IP address) of the person while making the change d. The information that was changed e. The outcome of the event f. The data before and after it was changed, and which screens were accessed and used
28	General System Behavior	Audit_&_Compliance	Any technology vendor, application or solution shall prevent modifications to the audit records.
29	General System Behavior	Audit_&_Compliance	Any technology vendor, application or solution must have the ability to capture electronic signatures on all documents, forms, letters, and correspondences.
30	General System Behavior	Audit_&_Compliance	Any technology vendor, application or solution shall be able to detect security-relevant events (as defined in NIST 800-53 moderate baseline, rev 4) that it mediates and generate audit records for them. At a minimum the events will include, but not be limited to: a. Start/stop b. User login/logout c. Session timeout d. Account lockout e. Client record created/viewed/updated/deleted f. Scheduling g. Query h. Order i. Node-authentication failure j. Signature created/validated k. Personally Identifiable Information (PII) export l. PII import m. Security administration events n. Backup and restore o. Audit Event Types listed in IRS 1075
31	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution interfaces will secure and protect (encrypt) the data and the associated infrastructure from a confidentiality, integrity and availability perspective.
32	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall develop/integrate services using standardized Web Services formats.

33	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall provide the ability to publish services and related data to be used by different types and classes of service consumers.
34	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall provide the capabilities for a Real-Time (or near real-time) Integrated Enterprise where common data elements about the customers served (e.g., clients) and services rendered are easily shared across organizational units with appropriate adherence to State and Federal security and privacy restrictions.
35	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall have the capability to implement synchronous and asynchronous program-to-program communication, moving messages between service oriented architecture (SOA) service consumer modules and service provider modules at runtime.
36	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall have message and data formats that will be based on logical representations of business objects rather than native application data structures.
37	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall avoid point-to-point integrations. Application integration, both internal and external, will go through the DHS Enterprise Service Bus/Data Integration Hub.
38	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution WSDLs developed for Arkansas will conform to the W3C standards for restful API development.
39	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution design will allow for the solution to continue to operate despite failure or unavailability of one or more individual technology solution components.
40	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall have the ability to use standards-based communication protocols, such as TCP/IP, HTTP, HTTP/S and SMTP. Protocol bridging: The ability to convert between the protocol native to the messaging platform and other protocols, such as Remote Method Invocation (RMI), IIOP and .NET remoting.
41	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution will have the capability to work with security policy manager for Web services that allows for centrally defined security policies that govern Web services operations (such as access policy, logging policy, and load balancing).
42	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall have the capability to integrate with Master Data Management (MDM) technology for Enterprise Master Client Index (EMCI) implemented as part of the "State Hub" in a centralized or registry style implementation.
43	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall be responsive and will automatically be sized for an optimum view to the display dimensions of PC, Tablet or Mobile phone.
44	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution components will be committed to an advanced approach to interoperability using web services and Service Oriented Architecture (SOA) aligned with DHS Enterprise Architecture Standards and industry standards and vision for interoperability.
45	General System Behavior	Perf. and Avail.	Any technology vendor, application or solution must be architected to support replication of the virtual machines to a secondary site.
46	General System Behavior	Perf. and Avail.	Any technology vendor, application or solution must be designed so all releases can be performed between 7pm and 6am except critical releases
47	General System Behavior	Perf. and Avail.	Any technology vendor, application or solution shall leverage virtualization to expedite disaster recovery. Virtualization enables system owners to quickly reconfigure system platforms without having to acquire additional hardware.
48	General System Behavior	Perf. and Avail.	Any technology vendor, application or solution will provide the ability to perform archival/incremental backups and the ability to perform open/closed database backups.
49	General System Behavior	Perf. and Avail.	Any technology vendor, application or solution will provide at least one (1) production and one (1) non-production environment. Highly available solutions that mitigate single points of failure are recommended and encouraged.
50	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall allow for different roles for Users including Operators, Administrators, Managers etc.

51	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall, at a minimum, provide a mechanism to comply with security requirements and safeguard requirements of the following Federal agencies / entities: a. Health & Human Services (HHS) Centers for Medicare & Medicaid Services (CMS) b. Guidance from CMS including MITA Framework 3.0 and Harmonized Security and Privacy Framework c. Administration for Children & Families (ACF) d. Dept. of Agriculture Food and Nutrition Services e. NIST 800-53 r4, MARS-E and DOD 8500.2 f. IRS pub 1075, which points back to NIST 800-53 rev 3 g. Federal Information Security Management Act (FISMA) of 2002 h. Health Insurance Portability and Accountability Act (HIPAA) of 1996 i. Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009 j. Privacy Act of 1974 k. e-Government Act of 2002 l. Patient Protection and Affordable Care Act of 2010, Section 1561 Recommendations m. Section 471(a)(8) of the Social Security Act n. Section 106(b)(2)(B)(viii) of the Child Abuse Prevention and Treatment Act
52	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall adhere to the accessibility standard as outlined in the web guidelines and based on the W3C level 2 accessibility guidelines: (http://www.w3.org/TR/WCAG10/full-checklist.html)
53	General System Behavior	Regulatory & Usability	Any technology vendor, application or solution shall adhere to the AR State accessibility standards and comply with the provisions of Arkansas Code Annotated § 25-26-201 et seq., as amended by Act 308 of 2013.
54	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution comply with the DHS branding standards as defined by DHS.
55	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall adhere to the principle of “Fail Safe” to ensure that a system in a failed state does not reveal any sensitive information or leave any access controls open for attacks
56	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall maintain a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of information
57	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall follow the DHS Enterprise Architecture Standards regarding identity, authorization and access management. The current standards state that applications/solutions will integrate with Microsoft's Active Directory for internal/DHS users and will integrate with the IBM Cloud Identity platform for external users. Modern authentication protocols such as SAML or OIDC should be used and multi-factor authentication will be employed whenever deemed necessary by DHS or applicable regulatory bodies (CMS, FNS, IRS, etc.).
58	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall support protection of confidentiality of all Protected Health Information (PHI) and Personally Identifiable Information (PII) delivered over the Internet or other known open networks via supported encryption technologies needed to meet CMS and NIST requirements for encryption of PHI and PII data. Examples include: Advanced Encryption Standard (AES) and an open protocol such as Transport Layer Security (TLS), Secure Sockets Layer (SSL), Internet Protocol Security (IPsec), XML encryptions, or Secure/Multipurpose Internet Mail Extensions (S/MIME) or their successors. All vendors, applications and solutions will be subject to external Audit checks.
59	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall, when storing PHI/PII, support the use of encryption technologies needed to meet CMS and NIST requirements for the encryption of PHI/PII data at rest.
60	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution, prior to accessing any PHI, display a State-approved configurable warning or login banner (e.g. "The System should only be accessed by authorized users"). In the event that a application or solution does not support pre-login capabilities, the application or solution will display the banner immediately following authorization.
61	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall not transmit or store any Personal Health Information (PHI) or Personally Identifiable Information (PII) using publically available storage over the Internet or any wireless communication device, unless: 1) the PHI or PII is “de-identified” in accordance with 45 C.F.R § 164.514(b) (2); or 2) encrypted in accordance with applicable law, including the American Recovery and Reinvestment Act of 2009 and as required by policies, procedures and standards established by DHS

62	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution will include the same security provisions for the development, System test, Acceptance test and training environment as those used in the production environment except those provisions implemented specifically to protect confidential information (e.g. PHI, PII).
63	general System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall be able to associate permissions with a user using one or more of the following access controls: a. Role-Based Access Controls (RBAC; users are grouped by role and access rights assigned to these groups) b. Context-based (role-based with additional access rights assigned or restricted based on the context of the transaction such as time-of-day, workstation-location, emergency-mode, etc.)
64	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution will comply with accessibility requirements described in 45 CFR 85 and with State of Arkansas accessibility requirements
65	General System Behavior	Solution Administration	Any technology vendor, application or solution will allow System administrators to create and manage user roles.
66	General System Behavior	Solution Administration	Any technology vendor, application or solution communications will be protected by at least 256-bit encryption.
67	General System Behavior	Solution Administration	Any technology vendor, application or solution will be supported by public key/private key encryption Secure Socket Layer (SSL) certificates.
68	General System Behavior	Regulatory & Usability	Any application or solution will use colors to enhance user experience and System usability while complying with all disability requirements notated elsewhere in these requirements.
69	General System Behavior	User Interrace	Any technology vendor, application or solution must perform address validation for demographic information (e.g., USPS, Smarty Streets, AR GIS, etc.). Suggest the validated new address and prompt user to select either user entered address or validated address and then save accordingly.
70	General System Behavior	User Interface	Any technology vendor, application or solution must perform standard data validations such as character, numeric, date, currency , phone, SSN etc.
71	General System Behavior	User Interlace	Any technology vendor, application or solution must have the ability to auto-save, prompt to save when leaving pages in all modules.
72	General System Behavior	User Interlace	Any technology vendor, application or solution shall have the ability to create prompts for user actions. (e.g., incomplete data entry of required fields, deletion of data, system log-off warnings).
73	General System Behavior	User Interlace	Any technology vendor, application or solution shall have the capability to send notifications. Examples include sending emails, text messages (SMS), etc.
74	General System Behavior	Web based UI	Any technology vendor, application or solution providing data over a web browser interface (http, ftp, etc.) will include the capability to encrypt the data communicated over the network via SSL (e.g.. HTML over HTTPS).
75	General System Behavior	Web based UI	The system will support and maintain compatibility with the current to (N-2) version of the DHS Support Operating Systems. The supported Operating Systems are Microsoft Windows, MAC OS, Apple IOS and Google Android.
76	General System Behavior	Web based UI	The system will support and maintain compatibility with the current to (N-2) version of the DHS approved Browsers. The supported Browsers are Chrome, Edge, and Safari. This is to ensure that vendors test and certify their software/application for current to (N-2) versions of these Browsers.
77	Technology Platform Requirements	Data Integ,Quality, ETL	Any technology vendor, application or solution Extract Transform and Load (ETL) components will provide process flow and user interface capabilities to enable business users to perform data-quality-related tasks and fulfill stewardship functions, including: a. Packaged processes, including steps used to perform common quality tasks (providing values for incomplete data, resolving conflicts of duplicate records, specifying custom rules for merging records, profiling, auditing, for example) b. User interface in which quality processes and issues are exposed to business users, stewards and others c. Functionality to manage the data quality issue resolution process through the stewardship workflow (status tracking, escalation and monitoring of the issue resolution process) d. Ability to customize the user interface and workflow of the resolution process e. Ability to execute data quality resolution steps in the context of a process orchestrated by Business Process Management (BPM) tools (packaged integration or other ability to work with popular BPM suites, for example)