STATE OF UTAH COOPERATIVE CONTRACT AMENDMENT

AMENDMENT #: 1

CONTRACT #: AR3087

Starting Date: 3/27/2019

Expiration Date: 9/15/2026

TO BE ATTACHED AND MADE PART OF the specified contract by and between the State of Utah Division of Purchasing and Armedia LLC (Referred to as CONTRACTOR).

BOTH PARTIES AGREE TO AMEND THE CONTRACT AS FOLLOWS:

Extend the contract 120 days. The new expiration date will be January 13th, 2027.

Effective Date of Amendment: Upon signature of both parties.

All other terms and conditions of the contract, including those previously modified, shall remain in full force and effect.

IN WITNESS WHEREOF, the parties sign and cause this contract to be executed.

CONTRACTOR

James Bailey (Aug 25, 2026 18:24:29 EDT) 08/25/2026

Contractor's Signature Date

James Bailey

Contractor's Name (Print)

CEO

Title (Print)

STATE OF UTAH

08/25/2026

Director, State of Utah Division of Purchasing Date

For Division of Purchasing Internal Use			
Purchasing Agent	Phone #	E-mail Address	**Contract #**
Keli Lessing	801-957-7167	klessing@utah.gov	AR3087

Contract #: AR3087

STATE OF UTAH COOPERATIVE CONTRACT

1. CONTRACTING PARTIES: This contract is between the Utah Division of Purchasing and the following Contractor:

Armedia, LLC
Name

8221 Old Courthouse Road, Suite 300
Street Address

Vienna	VA	22182
City	*State*	*Zip*

Vendor # VC226518 Commodity Code #: 920-05 Legal Status of Contractor: Limited Liability Company

Contact *Name:* James Bailey *Phone Number:* 703-272-3270 *Email:* james.bailey@armedia.com

2. CONTRACT PORTFOLIO NAME: Cloud Solutions.

3. GENERAL PURPOSE OF CONTRACT: Provide Cloud Solutions under the service models awarded in Attachment B.

4. PROCUREMENT: This contract is entered into as a result of the procurement process on FY2018, Solicitation# SK18008

5. CONTRACT PERIOD: Effective Date: Wednesday, March 27, 2019. Termination Date: Tuesday, September 15, 2026 unless terminated early or extended in accordance with the terms and conditions of this contract.

6. Administrative Fee: Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) of contract sales no later than 60 days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on sales of the Services.

7. ATTACHMENT A: NASPO ValuePoint Master Terms and Conditions, including the attached Exhibits
ATTACHMENT B: Scope of Services Awarded to Contractor
ATTACHMENT C: Pricing Discounts and Schedule
ATTACHMENT D: Contractor's Response to Solicitation # SK18008
ATTACHMENT E: Service Offering EULAs, SLAs

Any conflicts between Attachment A and the other Attachments will be resolved in favor of Attachment A.

9. DOCUMENTS INCORPORATED INTO THIS CONTRACT BY REFERENCE BUT NOT ATTACHED:
   a. All other governmental laws, regulations, or actions applicable to the goods and/or services authorized by this contract.
   b. Utah Procurement Code, Procurement Rules, and Contractor's response to solicitation #SK18008.

10. Each signatory below represents that he or she has the requisite authority to enter into this contract.

IN WITNESS WHEREOF, the parties sign and cause this contract to be executed. Notwithstanding verbal or other representations by the parties, the "Effective Date" of this Contract shall be the date provided within Section 5 above.

CONTRACTOR

James Bailey — Mar 28, 2019
James Bailey (Mar 28, 2019)
Contractor's signature — Date

James Bailey — President & CEO
Type or Print Name and Title

DIVISION OF PURCHASING

Christopher Hughes — Mar 29, 2019
Christopher Hughes (Mar 29, 2019)
Director, Division of Purchasing — Date

Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions

1. Master Agreement Order of Precedence

a. Any Order placed under this Master Agreement shall consist of the following documents:

(1) A Participating Entity's Participating Addendum[1] ("PA");
(2) NASPO ValuePoint Master Agreement Terms & Conditions, including the applicable Exhibits[2] to the Master Agreement;
(3) The Solicitation;
(4) Contractor's response to the Solicitation, as revised (if permitted) and accepted by the Lead State; and
(5) A Service Level Agreement issued against the Participating Addendum.

b. These documents shall be read to be consistent and complementary. Any conflict among these documents shall be resolved by giving priority to these documents in the order listed above. Contractor terms and conditions that apply to this Master Agreement are only those that are expressly accepted by the Lead State and must be in writing and attached to this Master Agreement as an Exhibit or Attachment.

2. Definitions - Unless otherwise provided in this Master Agreement, capitalized terms will have the meanings given to those terms in this Section.

Confidential Information means any and all information of any form that is marked as confidential or would by its nature be deemed confidential obtained by Contractor or its employees or agents in the performance of this Master Agreement, including, but not necessarily limited to (1) any Purchasing Entity's records, (2) personnel records, and (3) information concerning individuals, is confidential information of Purchasing Entity.

Contractor means the person or entity providing solutions under the terms and conditions set forth in this Master Agreement. Contractor also includes its employees, subcontractors, agents and affiliates who are providing the services agreed to under the Master Agreement.

Data means all information, whether in oral or written (including electronic) form,

[1] A Sample Participating Addendum will be published after the contracts have been awarded.
[2] The Exhibits comprise the terms and conditions for the service models: PaaS, IaaS, and PaaS.

created by or in any way originating with a Participating Entity or Purchasing Entity, and all information that is the output of any computer processing, or other electronic manipulation, of any information that was created by or in any way originating with a Participating Entity or Purchasing Entity, in the course of using and configuring the Services provided under this Agreement.

Data Breach means any actual or reasonably suspected non-authorized access to or acquisition of computerized Non-Public Data or Personal Data that compromises the security, confidentiality, or integrity of the Non-Public Data or Personal Data, or the ability of Purchasing Entity to access the Non-Public Data or Personal Data.

Data Categorization means the process of risk assessment of Data. See also “High Risk Data”, “Moderate Risk Data” and “Low Risk Data”.

Disabling Code means computer instructions or programs, subroutines, code, instructions, data or functions, (including but not limited to viruses, worms, date bombs or time bombs), including but not limited to other programs, data storage, computer libraries and programs that self-replicate without manual intervention, instructions programmed to activate at a predetermined time or upon a specified event, and/or programs purporting to do a meaningful function but designed for a different function, that alter, destroy, inhibit, damage, interrupt, interfere with or hinder the operation of the Purchasing Entity’s’ software, applications and/or its end users processing environment, the system in which it resides, or any other software or data on such system or any other system with which it is capable of communicating.

Fulfillment Partner means a third-party contractor qualified and authorized by Contractor, and approved by the Participating State under a Participating Addendum, who may, to the extent authorized by Contractor, fulfill any of the requirements of this Master Agreement including but not limited to providing Services under this Master Agreement and billing Customers directly for such Services. Contractor may, upon written notice to the Participating State, add or delete authorized Fulfillment Partners as necessary at any time during the contract term. Fulfillment Partner has no authority to amend this Master Agreement or to bind Contractor to any additional terms and conditions.

High Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems (“High Impact Data”).

Infrastructure as a Service (IaaS) as used in this Master Agreement is defined the capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Intellectual Property means any and all patents, copyrights, service marks, trademarks, trade secrets, trade names, patentable inventions, or other similar proprietary rights, in tangible or intangible form, and all rights, title, and interest therein.

Lead State means the State centrally administering the solicitation and any resulting Master Agreement(s).

Low Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems ("Low Impact Data").

Master Agreement means this agreement executed by and between the Lead State, acting on behalf of NASPO ValuePoint, and the Contractor, as now or hereafter amended.

Moderate Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems ("Moderate Impact Data").

NASPO ValuePoint is the NASPO ValuePoint Cooperative Purchasing Program, facilitated by the NASPO Cooperative Purchasing Organization LLC, a 501(c)(3) limited liability company (doing business as NASPO ValuePoint) is a subsidiary organization the National Association of State Procurement Officials (NASPO), the sole member of NASPO ValuePoint. The NASPO ValuePoint Cooperative Purchasing Organization facilitates administration of the cooperative group contracting consortium of state chief procurement officials for the benefit of state departments, institutions, agencies, and political subdivisions and other eligible entities (i.e., colleges, school districts, counties, cities, some nonprofit organizations, etc.) for all states and the District of Columbia. The NASPO ValuePoint Cooperative Development Team is identified in the Master Agreement as the recipient of reports and may be performing contract administration functions as assigned by the Lead State.

Non-Public Data means High Risk Data and Moderate Risk Data that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the Purchasing Entity because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

Participating Addendum means a bilateral agreement executed by a Contractor and a Participating Entity incorporating this Master Agreement and any other additional Participating Entity specific language or other requirements, e.g. ordering procedures specific to the Participating Entity, other terms and conditions.

Participating Entity means a state, or other legal entity, properly authorized to enter into a Participating Addendum.

Participating State means a state, the District of Columbia, or one of the territories of the United States that is listed in the Request for Proposal as intending to participate.

Upon execution of the Participating Addendum, a Participating State becomes a Participating Entity.

Personal Data means data alone or in combination that includes information relating to an individual that identifies the individual by name, identifying number, mark or description can be readily associated with a particular individual and which is not a public record. Personal Information may include the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, passport); financial account information, including account number, credit or debit card numbers; or Protected Health Information (PHI) relating to a person.

Platform as a Service (PaaS) as used in this Master Agreement is defined as the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or -acquired applications created using programming languages and tools supported by the provider. This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Product means any deliverable under this Master Agreement, including Services, software, and any incidental tangible goods.

Protected Health Information (PHI) means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer. PHI may also include information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Purchasing Entity means a state, city, county, district, other political subdivision of a State, and a nonprofit organization under the laws of some states if authorized by a Participating Addendum, who issues a Purchase Order against the Master Agreement and becomes financially committed to the purchase.

Services mean any of the specifications described in the Scope of Services that are supplied or created by the Contractor pursuant to this Master Agreement.

Security Incident means the possible or actual unauthorized access to a Purchasing

Entity's Non-Public Data and Personal Data the Contractor believes could reasonably result in the use, disclosure or theft of a Purchasing Entity's Non-Public Data within the possession or control of the Contractor. A Security Incident also includes a major security breach to the Contractor's system, regardless if Contractor is aware of unauthorized access to a Purchasing Entity's Non-Public Data. A Security Incident may or may not turn into a Data Breach.

Service Level Agreement (SLA) means a written agreement between both the Purchasing Entity and the Contractor that is subject to the terms and conditions in this Master Agreement and relevant Participating Addendum unless otherwise expressly agreed in writing between the Purchasing Entity and the Contractor. SLAs should include: (1) the technical service level performance promises, (i.e. metrics for performance and intervals for measure), (2) description of service quality, (3) identification of roles and responsibilities, (4) remedies, such as credits, and (5) an explanation of how remedies or credits are calculated and issued.

Software as a Service (SaaS) as used in this Master Agreement is defined as the capability provided to the consumer to use the Contractor's applications running on a Contractor's infrastructure (commonly referred to as 'cloud infrastructure). The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Solicitation means the documents used by the State of Utah, as the Lead State, to obtain Contractor's Proposal.

Statement of Work means a written statement in a solicitation document or contract that describes the Purchasing Entity's service needs and expectations.

3. Term of the Master Agreement: Unless otherwise specified as a shorter term in a Participating Addendum, the term of the Master Agreement will run from contract execution to September 15, 2026.

4. Amendments: The terms of this Master Agreement shall not be waived, altered, modified, supplemented or amended in any manner whatsoever without prior written approval of the Lead State and Contractor.

5. Assignment/Subcontracts: Contractor shall not assign, sell, transfer, or sublet rights, or delegate responsibilities under this Master Agreement, in whole or in part, without the prior written approval of the Lead State.

The Lead State reserves the right to assign any rights or duties, including written assignment of contract administration duties to the NASPO Cooperative Purchasing Organization LLC, doing business as NASPO ValuePoint.

6. Discount Guarantee Period: All discounts must be guaranteed for the entire term of the Master Agreement. Participating Entities and Purchasing Entities shall receive the immediate benefit of price or rate reduction of the services provided under this Master Agreement. A price or rate reduction will apply automatically to the Master Agreement and an amendment is not necessary.

7. Termination: Unless otherwise stated, this Master Agreement may be terminated by either party upon 60 days written notice prior to the effective date of the termination. Further, any Participating Entity may terminate its participation upon 30 days written notice, unless otherwise limited or stated in the Participating Addendum. Termination may be in whole or in part. Any termination under this provision shall not affect the rights and obligations attending orders outstanding at the time of termination, including any right of any Purchasing Entity to indemnification by the Contractor, rights of payment for Services delivered and accepted, data ownership, Contractor obligations regarding Purchasing Entity Data, rights attending default in performance an applicable Service Level of Agreement in association with any Order, Contractor obligations under Termination and Suspension of Service, and any responsibilities arising out of a Security Incident or Data Breach. Termination of the Master Agreement due to Contractor default may be immediate.

8. Confidentiality, Non-Disclosure, and Injunctive Relief

a. Confidentiality. Contractor acknowledges that it and its employees or agents may, in the course of providing a Product under this Master Agreement, be exposed to or acquire information that is confidential to Purchasing Entity's or Purchasing Entity's clients. Any reports or other documents or items (including software) that result from the use of the Confidential Information by Contractor shall be treated in the same manner as the Confidential Information. Confidential Information does not include information that (1) is or becomes (other than by disclosure by Contractor) publicly known; (2) is furnished by Purchasing Entity to others without restrictions similar to those imposed by this Master Agreement; (3) is rightfully in Contractor's possession without the obligation of nondisclosure prior to the time of its disclosure under this Master Agreement; (4) is obtained from a source other than Purchasing Entity without the obligation of confidentiality, (5) is disclosed with the written consent of Purchasing Entity or; (6) is independently developed by employees, agents or subcontractors of Contractor who can be shown to have had no access to the Confidential Information.

b. Non-Disclosure. Contractor shall hold Confidential Information in confidence, using at least the industry standard of confidentiality, and shall not copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give, or disclose Confidential Information to third parties or use Confidential Information for any purposes whatsoever other than what is necessary to the performance of Orders placed under this Master Agreement. Contractor shall advise each of its employees and agents of their obligations to keep Confidential Information confidential. Contractor shall use commercially reasonable efforts to assist Purchasing Entity in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the generality of the foregoing, Contractor shall advise Purchasing Entity, applicable Participating Entity, and the Lead State immediately if Contractor learns or has reason

to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Master Agreement, and Contractor shall at its expense cooperate with Purchasing Entity in seeking injunctive or other equitable relief in the name of Purchasing Entity or Contractor against any such person. Except as directed by Purchasing Entity, Contractor will not at any time during or after the term of this Master Agreement disclose, directly or indirectly, any Confidential Information to any person, except in accordance with this Master Agreement, and that upon termination of this Master Agreement or at Purchasing Entity's request, Contractor shall turn over to Purchasing Entity all documents, papers, and other matter in Contractor's possession that embody Confidential Information. Notwithstanding the foregoing, Contractor may keep one copy of such Confidential Information necessary for quality assurance, audits and evidence of the performance of this Master Agreement.

c. Injunctive Relief. Contractor acknowledges that breach of this section, including disclosure of any Confidential Information, will cause irreparable injury to Purchasing Entity that is inadequately compensable in damages. Accordingly, Purchasing Entity may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies that may be available. Contractor acknowledges and agrees that the covenants contained herein are necessary for the protection of the legitimate business interests of Purchasing Entity and are reasonable in scope and content.

d. Purchasing Entity Law. These provisions shall be applicable only to extent they are not in conflict with the applicable public disclosure laws of any Purchasing Entity.

9. Right to Publish: Throughout the duration of this Master Agreement, Contractor must secure prior approval from the Lead State or Participating Entity for the release of any information that pertains to the potential work or activities covered by the Master Agreement , including but not limited to reference to or use of the Lead State or a Participating Entity's name, Great Seal of the State, Coat of Arms, any Agency or other subunits of the State government, or any State official or employee, for commercial promotion which is strictly prohibited. News releases or release of broadcast e-mails pertaining to this Master Agreement or Participating Addendum shall not be made without prior written approval of the Lead State or a Participating Entity.

The Contractor shall not make any representations of NASPO ValuePoint's opinion or position as to the quality or effectiveness of the services that are the subject of this Master Agreement without prior written consent. Failure to adhere to this requirement may result in termination of the Master Agreement for cause.

10. Defaults and Remedies

a. The occurrence of any of the following events shall be an event of default under this Master Agreement:

(1) Nonperformance of contractual requirements; or

(2) A material breach of any term or condition of this Master Agreement; or

(3) Any certification, representation or warranty by Contractor in response to the

solicitation or in this Master Agreement that proves to be untrue or materially misleading; or

(4) Institution of proceedings under any bankruptcy, insolvency, reorganization or similar law, by or against Contractor, or the appointment of a receiver or similar officer for Contractor or any of its property, which is not vacated or fully stayed within thirty (30) calendar days after the institution or occurrence thereof; or

(5) Any default specified in another section of this Master Agreement.

b. Upon the occurrence of an event of default, Lead State shall issue a written notice of default, identifying the nature of the default, and providing a period of 30 calendar days in which Contractor shall have an opportunity to cure the default. The Lead State shall not be required to provide advance written notice or a cure period and may immediately terminate this Master Agreement in whole or in part if the Lead State, in its sole discretion, determines that it is reasonably necessary to preserve public safety or prevent immediate public crisis. Time allowed for cure shall not diminish or eliminate Contractor's liability for damages.

c. If Contractor is afforded an opportunity to cure and fails to cure the default within the period specified in the written notice of default, Contractor shall be in breach of its obligations under this Master Agreement and Lead State shall have the right to exercise any or all of the following remedies:

(1) Exercise any remedy provided by law; and

(2) Terminate this Master Agreement and any related Contracts or portions thereof; and

(3) Suspend Contractor from being able to respond to future bid solicitations; and

(4) Suspend Contractor's performance; and

(5) Withhold payment until the default is remedied.

d. Unless otherwise specified in the Participating Addendum, in the event of a default under a Participating Addendum, a Participating Entity shall provide a written notice of default as described in this section and have all of the rights and remedies under this paragraph regarding its participation in the Master Agreement, in addition to those set forth in its Participating Addendum. Nothing in these Master Agreement Terms and Conditions shall be construed to limit the rights and remedies available to a Purchasing Entity under the applicable commercial code.

11. Changes in Contractor Representation: The Contractor must notify the Lead State of changes in the Contractor's key administrative personnel, in writing within 10 calendar days of the change. The Lead State reserves the right to approve changes in key personnel, as identified in the Contractor's proposal. The Contractor agrees to propose replacement key personnel having substantially equal or better education, training, and experience as was possessed by the key person proposed and evaluated in the Contractor's proposal.

12. Force Majeure: Neither party shall be in default by reason of any failure in

performance of this Contract in accordance with reasonable control and without fault or negligence on their part. Such causes may include, but are not restricted to, acts of nature or the public enemy, acts of the government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, freight embargoes and unusually severe weather, but in every case the failure to perform such must be beyond the reasonable control and without the fault or negligence of the party.

13. Indemnification

a. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, and Purchasing Entities, along with their officers, agents, and employees as well as any person or entity for which they may be liable, from and against claims, damages or causes of action including reasonable attorneys' fees and related costs for any death, injury, or damage to property arising directly or indirectly from act(s), error(s), or omission(s) of the Contractor, its employees or subcontractors or volunteers, at any tier, relating to the performance under the Master Agreement.

b. Indemnification – Intellectual Property. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, Purchasing Entities, along with their officers, agents, and employees as well as any person or entity for which they may be liable ("Indemnified Party"), from and against claims, damages or causes of action including reasonable attorneys' fees and related costs arising out of the claim that the Product or its use, infringes Intellectual Property rights ("Intellectual Property Claim") of another person or entity.

(1) The Contractor's obligations under this section shall not extend to any claims arising from the combination of the Product with any other product, system or method, unless the Product, system or method is:

(a) provided by the Contractor or the Contractor's subsidiaries or affiliates;

(b) specified by the Contractor to work with the Product; or

(c) reasonably required, in order to use the Product in its intended manner, and the infringement could not have been avoided by substituting another reasonably available product, system or method capable of performing the same function; or

(d) It would be reasonably expected to use the Product in combination with such product, system or method.

(2) The Indemnified Party shall notify the Contractor within a reasonable time after receiving notice of an Intellectual Property Claim. Even if the Indemnified Party fails to provide reasonable notice, the Contractor shall not be relieved from its obligations unless the Contractor can demonstrate that it was prejudiced in defending the Intellectual Property Claim resulting in increased expenses or loss to the Contractor and then only to the extent of the prejudice or expenses. If the Contractor promptly and

reasonably investigates and defends any Intellectual Property Claim, it shall have control over the defense and settlement of it. However, the Indemnified Party must consent in writing for any money damages or obligations for which it may be responsible. The Indemnified Party shall furnish, at the Contractor's reasonable request and expense, information and assistance necessary for such defense. If the Contractor fails to vigorously pursue the defense or settlement of the Intellectual Property Claim, the Indemnified Party may assume the defense or settlement of it and the Contractor shall be liable for all costs and expenses, including reasonable attorneys' fees and related costs, incurred by the Indemnified Party in the pursuit of the Intellectual Property Claim. Unless otherwise agreed in writing, this section is not subject to any limitations of liability in this Master Agreement or in any other document executed in conjunction with this Master Agreement.

14. Independent Contractor: The Contractor shall be an independent contractor. Contractor shall have no authorization, express or implied, to bind the Lead State, Participating States, other Participating Entities, or Purchasing Entities to any agreements, settlements, liability or understanding whatsoever, and agrees not to hold itself out as agent except as expressly set forth herein or as expressly agreed in any Participating Addendum.

15. Individual Customers: Except to the extent modified by a Participating Addendum, each Purchasing Entity shall follow the terms and conditions of the Master Agreement and applicable Participating Addendum and will have the same rights and responsibilities for their purchases as the Lead State has in the Master Agreement, including but not limited to, any indemnity or right to recover any costs as such right is defined in the Master Agreement and applicable Participating Addendum for their purchases. Each Purchasing Entity will be responsible for its own charges, fees, and liabilities. The Contractor will apply the charges and invoice each Purchasing Entity individually.

16. Insurance

a. Unless otherwise agreed in a Participating Addendum, Contractor shall, during the term of this Master Agreement, maintain in full force and effect, the insurance described in this section. Contractor shall acquire such insurance from an insurance carrier or carriers licensed to conduct business in each Participating Entity's state and having a rating of A-, Class VII or better, in the most recently published edition of Best's Reports. Failure to buy and maintain the required insurance may result in this Master Agreement's termination or, at a Participating Entity's option, result in termination of its Participating Addendum.

b. Coverage shall be written on an occurrence basis. The minimum acceptable limits shall be as indicated below, with no deductible for each of the following categories:

(1) Commercial General Liability covering premises operations, independent contractors, products and completed operations, blanket contractual liability, personal injury (including death), advertising liability, and property damage, with a limit of not less than $1 million per occurrence/$3 million general

aggregate;

(2) CLOUD MINIMUM INSURANCE COVERAGE:

Level of Risk	**Data Breach and Privacy/Cyber Liability including Technology Errors and Omissions** Minimum Insurance Coverage
Low Risk Data	$2,000,000
Moderate Risk Data	$5,000,000
High Risk Data	$10,000,000

(3) Contractor must comply with any applicable State Workers Compensation or Employers Liability Insurance requirements.

(4) Professional Liability. As applicable, Professional Liability Insurance Policy in the minimum amount of $1,000,000 per occurrence and $1,000,000 in the aggregate, written on an occurrence form that provides coverage for its work undertaken pursuant to each Participating Addendum.

c. Contractor shall pay premiums on all insurance policies. Such policies shall also reference this Master Agreement and shall have a condition that they not be revoked by the insurer until thirty (30) calendar days after notice of intended revocation thereof shall have been given to Purchasing Entity and Participating Entity by the Contractor.

d. Prior to commencement of performance, Contractor shall provide to the Lead State a written endorsement to the Contractor's general liability insurance policy or other documentary evidence acceptable to the Lead State that (1) names the Participating States identified in the Request for Proposal as additional insureds, (2) provides that no material alteration, cancellation, non-renewal, or expiration of the coverage contained in such policy shall have effect unless the named Participating State has been given at least thirty (30) days prior written notice, and (3) provides that the Contractor's liability insurance policy shall be primary, with any liability insurance of any Participating State as secondary and noncontributory. Unless otherwise agreed in any Participating Addendum, the Participating Entity's rights and Contractor's obligations are the same as those specified in the first sentence of this subsection. Before performance of any Purchase Order issued after execution of a Participating Addendum authorizing it, the Contractor shall provide to a Purchasing Entity or Participating Entity who requests it the same information described in this subsection.

e. Contractor shall furnish to the Lead State, Participating Entity, and, on request, the Purchasing Entity copies of certificates of all required insurance within thirty (30) calendar days of the execution of this Master Agreement, the execution of a Participating Addendum, or the Purchase Order's effective date and prior to performing any work. The insurance certificate shall provide the following information: the name and address of the insured; name, address, telephone number and signature of the authorized agent; name of the insurance company (authorized to operate in all states);

a description of coverage in detailed standard terminology (including policy period, policy number, limits of liability, exclusions and endorsements); and an acknowledgment of the requirement for notice of cancellation. Copies of renewal certificates of all required insurance shall be furnished within thirty (30) days after any renewal date. These certificates of insurance must expressly indicate compliance with each and every insurance requirement specified in this section. Failure to provide evidence of coverage may, at sole option of the Lead State, or any Participating Entity, result in this Master Agreement's termination or the termination of any Participating Addendum.

f. Coverage and limits shall not limit Contractor's liability and obligations under this Master Agreement, any Participating Addendum, or any Purchase Order.

17. Laws and Regulations: Any and all Services offered and furnished shall comply fully with all applicable Federal and State laws and regulations.

18. No Waiver of Sovereign Immunity: In no event shall this Master Agreement, any Participating Addendum or any contract or any Purchase Order issued thereunder, or any act of a Lead State, a Participating Entity, or a Purchasing Entity be a waiver of any form of defense or immunity, whether sovereign immunity, governmental immunity, immunity based on the Eleventh Amendment to the Constitution of the United States or otherwise, from any claim or from the jurisdiction of any court.

This section applies to a claim brought against the Participating State only to the extent Congress has appropriately abrogated the Participating State's sovereign immunity and is not consent by the Participating State to be sued in federal court. This section is also not a waiver by the Participating State of any form of immunity, including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

19. Ordering

a. Master Agreement order and purchase order numbers shall be clearly shown on all acknowledgments, shipping labels, packing slips, invoices, and on all correspondence.

b. This Master Agreement permits Purchasing Entities to define project-specific requirements and informally compete the requirement among other firms having a Master Agreement on an "as needed" basis. This procedure may also be used when requirements are aggregated or other firm commitments may be made to achieve reductions in pricing. This procedure may be modified in Participating Addenda and adapted to Purchasing Entity rules and policies. The Purchasing Entity may in its sole discretion determine which firms should be solicited for a quote. The Purchasing Entity may select the quote that it considers most advantageous, cost and other factors considered.

c. Each Purchasing Entity will identify and utilize its own appropriate purchasing procedure and documentation. Contractor is expected to become familiar with the Purchasing Entities' rules, policies, and procedures regarding the ordering of supplies and/or services contemplated by this Master Agreement.

d. Contractor shall not begin providing Services without a valid Service Level Agreement or other appropriate commitment document compliant with the law of the Purchasing Entity.

e. Orders may be placed consistent with the terms of this Master Agreement during the term of the Master Agreement.

f. All Orders pursuant to this Master Agreement, at a minimum, shall include:

(1) The services or supplies being delivered;
(2) The place and requested time of delivery;
(3) A billing address;
(4) The name, phone number, and address of the Purchasing Entity representative;
(5) The price per unit or other pricing elements consistent with this Master Agreement and the contractor's proposal;
(6) A ceiling amount of the order for services being ordered; and
(7) The Master Agreement identifier and the Participating State contract identifier.

g. All communications concerning administration of Orders placed shall be furnished solely to the authorized purchasing agent within the Purchasing Entity's purchasing office, or to such other individual identified in writing in the Order.

h. Orders must be placed pursuant to this Master Agreement prior to the termination date of this Master Agreement. Contractor is reminded that financial obligations of Purchasing Entities payable after the current applicable fiscal year are contingent upon agency funds for that purpose being appropriated, budgeted, and otherwise made available.

i. Notwithstanding the expiration or termination of this Master Agreement, Contractor agrees to perform in accordance with the terms of any Orders then outstanding at the time of such expiration or termination. Contractor shall not honor any Orders placed after the expiration or termination of this Master Agreement. Orders from any separate indefinite quantity, task orders, or other form of indefinite delivery order arrangement priced against this Master Agreement may not be placed after the expiration or termination of this Master Agreement, notwithstanding the term of any such indefinite delivery order agreement.

20. Participants and Scope

a. Contractor may not deliver Services under this Master Agreement until a Participating Addendum acceptable to the Participating Entity and Contractor is executed. The NASPO ValuePoint Master Agreement Terms and Conditions are applicable to any Order by a Participating Entity (and other Purchasing Entities covered by their Participating Addendum), except to the extent altered, modified, supplemented or amended by a Participating Addendum. By way of illustration and not limitation, this

authority may apply to unique delivery and invoicing requirements, confidentiality requirements, defaults on Orders, governing law and venue relating to Orders by a Participating Entity, indemnification, and insurance requirements. Statutory or constitutional requirements relating to availability of funds may require specific language in some Participating Addenda in order to comply with applicable law. The expectation is that these alterations, modifications, supplements, or amendments will be addressed in the Participating Addendum or, with the consent of the Purchasing Entity and Contractor, may be included in the ordering document (e.g. purchase order or contract) used by the Purchasing Entity to place the Order.

b. Subject to subsection 20c and a Participating Entity's Participating Addendum, the use of specific NASPO ValuePoint cooperative Master Agreements by state agencies, political subdivisions and other Participating Entities (including cooperatives) authorized by individual state's statutes to use state contracts is subject to the approval of the respective State Chief Procurement Official.

c. Unless otherwise stipulated in a Participating Entity's Participating Addendum, specific services accessed through the NASPO ValuePoint cooperative Master Agreements for Cloud Services by state executive branch agencies, as required by a Participating Entity's statutes, are subject to the authority and approval of the Participating Entity's Chief Information Officer's Office[3].

d. Obligations under this Master Agreement are limited to those Participating Entities who have signed a Participating Addendum and Purchasing Entities within the scope of those Participating Addenda. States or other entities permitted to participate may use an informal competitive process to determine which Master Agreements to participate in through execution of a Participating Addendum. Financial obligations of Participating States are limited to the orders placed by the departments or other state agencies and institutions having available funds. Participating States incur no financial obligations on behalf of political subdivisions.

e. NASPO ValuePoint is not a party to the Master Agreement. It is a nonprofit cooperative purchasing organization assisting states in administering the NASPO ValuePoint cooperative purchasing program for state government departments, institutions, agencies and political subdivisions (e.g., colleges, school districts, counties, cities, etc.) for all 50 states, the District of Columbia and the territories of the United States.

f. Participating Addenda shall not be construed to amend the terms of this Master Agreement between the Lead State and Contractor.

g. Participating Entities who are not states may under some circumstances sign their own Participating Addendum, subject to the approval of participation by the Chief Procurement Official of the state where the Participating Entity is located. Coordinate

[3] Chief Information Officer means the individual designated by the Governor with Executive Branch, enterprise-wide responsibility for the leadership and management of information technology resources of a state.

requests for such participation through NASPO ValuePoint. Any permission to participate through execution of a Participating Addendum is not a determination that procurement authority exists in the Participating Entity; they must ensure that they have the requisite procurement authority to execute a Participating Addendum.

h. Resale. Subject to any explicit permission in a Participating Addendum, Purchasing Entities may not resell goods, software, or Services obtained under this Master Agreement. This limitation does not prohibit: payments by employees of a Purchasing Entity as explicitly permitted under this agreement; sales of goods to the general public as surplus property; and fees associated with inventory transactions with other governmental or nonprofit entities under cooperative agreements and consistent with a Purchasing Entity's laws and regulations. Any sale or transfer permitted by this subsection must be consistent with license rights granted for use of intellectual property.

21. Payment: Orders under this Master Agreement are fixed-price or fixed-rate orders, not cost reimbursement contracts. Unless otherwise stipulated in the Participating Addendum, Payment is normally made within 30 days following the date of a correct invoice is received. Purchasing Entities reserve the right to withhold payment of a portion (including all if applicable) of disputed amount of an invoice. After 45 days the Contractor may assess overdue account charges up to a maximum rate of one percent per month on the outstanding balance. Payments will be remitted by mail. Payments may be made via a State or political subdivision "Purchasing Card" with no additional charge.

22. Data Access Controls: Contractor will provide access to Purchasing Entity's Data only to those Contractor employees, contractors and subcontractors ("Contractor Staff") who need to access the Data to fulfill Contractor's obligations under this Agreement. Contractor shall not access a Purchasing Entity's user accounts or Data, except on the course of data center operations, response to service or technical issues, as required by the express terms of this Master Agreement, or at a Purchasing Entity's written request.

Contractor may not share a Purchasing Entity's Data with its parent corporation, other affiliates, or any other third party without the Purchasing Entity's express written consent.

Contractor will ensure that, prior to being granted access to the Data, Contractor Staff who perform work under this Agreement have successfully completed annual instruction of a nature sufficient to enable them to effectively comply with all Data protection provisions of this Agreement; and possess all qualifications appropriate to the nature of the employees' duties and the sensitivity of the Data they will be handling.

23. Operations Management: Contractor shall maintain the administrative, physical, technical, and procedural infrastructure associated with the provision of the Product in a manner that is, at all times during the term of this Master Agreement, at a level equal to or more stringent than those specified in the Solicitation.

24. Public Information: This Master Agreement and all related documents are subject to disclosure pursuant to the Purchasing Entity's public information laws.

25. Purchasing Entity Data: Purchasing Entity retains full right and title to Data provided by it and any Data derived therefrom, including metadata.
Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. The obligation shall extend beyond the term of this Master Agreement in perpetuity.

Contractor shall not use any information collected in connection with this Master Agreement, including Purchasing Entity Data, for any purpose other than fulfilling its obligations under this Master Agreement.

26. Records Administration and Audit.

a. The Contractor shall maintain books, records, documents, and other evidence pertaining to this Master Agreement and orders placed by Purchasing Entities under it to the extent and in such detail as shall adequately reflect performance and administration of payments and fees. Contractor shall permit the Lead State, a Participating Entity, a Purchasing Entity, the federal government (including its grant awarding entities and the U.S. Comptroller General), and any other duly authorized agent of a governmental agency, to audit, inspect, examine, copy and/or transcribe Contractor's books, documents, papers and records directly pertinent to this Master Agreement or orders placed by a Purchasing Entity under it for the purpose of making audits, examinations, excerpts, and transcriptions. This right shall survive for a period of six (6) years following termination of this Agreement or final payment for any order placed by a Purchasing Entity against this Agreement, whichever is later, to assure compliance with the terms hereof or to evaluate performance hereunder.

b. Without limiting any other remedy available to any governmental entity, the Contractor shall reimburse the applicable Lead State, Participating Entity, or Purchasing Entity for any overpayments inconsistent with the terms of the Master Agreement or orders or underpayment of fees found as a result of the examination of the Contractor's records.

c. The rights and obligations herein exist in addition to any quality assurance obligation in the Master Agreement requiring the Contractor to self-audit contract obligations and that permits the Lead State to review compliance with those obligations.

d. The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement and applicable Participating Addendum terms. The purchasing entity may perform this audit or contract with a third party at its discretion and at the purchasing entity's expense.

27. Administrative Fees: The Contractor shall pay to NASPO ValuePoint, or its

assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) no later than 60 days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on sales of the Services. The NASPO ValuePoint Administrative Fee is not negotiable. This fee is to be included as part of the pricing submitted with proposal.

Additionally, some states may require an additional administrative fee be paid directly to the state on purchases made by Purchasing Entities within that state. For all such requests, the fee level, payment method and schedule for such reports and payments will be incorporated into the Participating Addendum that is made a part of the Master Agreement. The Contractor may adjust the Master Agreement pricing accordingly for purchases made by Purchasing Entities within the jurisdiction of the state. All such agreements shall not affect the NASPO ValuePoint Administrative Fee percentage or the prices paid by the Purchasing Entities outside the jurisdiction of the state requesting the additional fee. The NASPO ValuePoint Administrative Fee shall be based on the gross amount of all sales at the adjusted prices (if any) in Participating Addenda.

28. System Failure or Damage: In the event of system failure or damage caused by Contractor or its Services, the Contractor agrees to use its best efforts to restore or assist in restoring the system to operational capacity.

29. Title to Product: If access to the Product requires an application program interface (API), Contractor shall convey to Purchasing Entity an irrevocable and perpetual license to use the API.

30. Data Privacy: The Contractor must comply with all applicable laws related to data privacy and security, including IRS Pub 1075. Prior to entering into a SLA with a Purchasing Entity, the Contractor and Purchasing Entity must cooperate and hold a meeting to determine the Data Categorization to determine whether the Contractor will hold, store, or process High Risk Data, Moderate Risk Data and Low Risk Data. The Contractor must document the Data Categorization in the SLA or Statement of Work.

31. Warranty: At a minimum the Contractor must warrant the following:

a. Contractor has acquired any and all rights, grants, assignments, conveyances, licenses, permissions, and authorization for the Contractor to provide the Services described in this Master Agreement.

b. Contractor will perform materially as described in this Master Agreement, SLA, Statement of Work, including any performance representations contained in the Contractor's response to the Solicitation by the Lead State.

c. Contractor represents and warrants that the representations contained in its response to the Solicitation by the Lead State.

d. The Contractor will not interfere with a Purchasing Entity's access to and use of the

Services it acquires from this Master Agreement.

e. The Services provided by the Contractor are compatible with and will operate successfully with any environment (including web browser and operating system) specified by the Contractor in its response to the Solicitation by the Lead State.

f. The Contractor warrants that the Products it provides under this Master Agreement are free of malware. The Contractor must use industry-leading technology to detect and remove worms, Trojans, rootkits, rogues, dialers, spyware, etc.

32. Transition Assistance:

a. The Contractor shall reasonably cooperate with other parties in connection with all Services to be delivered under this Master Agreement, including without limitation any successor service provider to whom a Purchasing Entity's Data is transferred in connection with the termination or expiration of this Master Agreement. The Contractor shall assist a Purchasing Entity in exporting and extracting a Purchasing Entity's Data, in a format usable without the use of the Services and as agreed by a Purchasing Entity, at no additional cost to the Purchasing Entity. Any transition services requested by a Purchasing Entity involving additional knowledge transfer and support may be subject to a separate transition Statement of Work.

b. A Purchasing Entity and the Contractor shall, when reasonable, create a Transition Plan Document identifying the transition services to be provided and including a Statement of Work if applicable.

c. The Contractor must maintain the confidentiality and security of a Purchasing Entity's Data during the transition services and thereafter as required by the Purchasing Entity.

33. Waiver of Breach: Failure of the Lead State, Participating Entity, or Purchasing Entity to declare a default or enforce any rights and remedies shall not operate as a waiver under this Master Agreement or Participating Addendum. Any waiver by the Lead State, Participating Entity, or Purchasing Entity must be in writing. Waiver by the Lead State or Participating Entity of any default, right or remedy under this Master Agreement or Participating Addendum, or by Purchasing Entity with respect to any Purchase Order, or breach of any terms or requirements of this Master Agreement, a Participating Addendum, or Purchase Order shall not be construed or operate as a waiver of any subsequent default or breach of such term or requirement, or of any other term or requirement under this Master Agreement, Participating Addendum, or Purchase Order.

34. Assignment of Antitrust Rights: Contractor irrevocably assigns to a Participating Entity who is a state any claim for relief or cause of action which the Contractor now has or which may accrue to the Contractor in the future by reason of any violation of state or federal antitrust laws (15 U.S.C. § 1-15 or a Participating Entity's state antitrust provisions), as now in effect and as may be amended from time to time, in connection

with any goods or services provided to the Contractor for the purpose of carrying out the Contractor's obligations under this Master Agreement or Participating Addendum, including, at a Participating Entity's option, the right to control any such litigation on such claim for relief or cause of action.

35. Debarment : The Contractor certifies, to the best of its knowledge, that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction (contract) by any governmental department or agency. This certification represents a recurring certification made at the time any Order is placed under this Master Agreement. If the Contractor cannot certify this statement, attach a written explanation for review by the Lead State.

36. Performance and Payment Time Frames that Exceed Contract Duration: All maintenance or other agreements for services entered into during the duration of an SLA and whose performance and payment time frames extend beyond the duration of this Master Agreement shall remain in effect for performance and payment purposes (limited to the time frame and services established per each written agreement). No new leases, maintenance or other agreements for services may be executed after the Master Agreement has expired. For the purposes of this section, renewals of maintenance, subscriptions, SaaS subscriptions and agreements, and other service agreements, shall not be considered as "new."

37. Governing Law and Venue

a. The procurement, evaluation, and award of the Master Agreement shall be governed by and construed in accordance with the laws of the Lead State sponsoring and administering the procurement. The construction and effect of the Master Agreement after award shall be governed by the law of the state serving as Lead State (in most cases also the Lead State). The construction and effect of any Participating Addendum or Order against the Master Agreement shall be governed by and construed in accordance with the laws of the Participating Entity's or Purchasing Entity's State.

b. Unless otherwise specified in the RFP, the venue for any protest, claim, dispute or action relating to the procurement, evaluation, and award is in the Lead State. Venue for any claim, dispute or action concerning the terms of the Master Agreement shall be in the state serving as Lead State. Venue for any claim, dispute, or action concerning any Order placed against the Master Agreement or the effect of a Participating Addendum shall be in the Purchasing Entity's State.

c. If a claim is brought in a federal forum, then it must be brought and adjudicated solely and exclusively within the United States District Court for (in decreasing order of priority): the Lead State for claims relating to the procurement, evaluation, award, or contract performance or administration if the Lead State is a party; the Participating State if a named party; the Participating Entity state if a named party; or the Purchasing Entity state if a named party.

d. This section is also not a waiver by the Participating State of any form of immunity,

including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

38. No Guarantee of Service Volumes: The Contractor acknowledges and agrees that the Lead State and NASPO ValuePoint makes no representation, warranty or condition as to the nature, timing, quality, quantity or volume of business for the Services or any other products and services that the Contractor may realize from this Master Agreement, or the compensation that may be earned by the Contractor by offering the Services. The Contractor acknowledges and agrees that it has conducted its own due diligence prior to entering into this Master Agreement as to all the foregoing matters.

39. NASPO ValuePoint eMarket Center: In July 2011, NASPO ValuePoint entered into a multi-year agreement with JAGGAER, formerly SciQuest, whereby JAGGAER will provide certain electronic catalog hosting and management services to enable eligible NASPO ValuePoint's customers to access a central online website to view and/or shop the goods and services available from existing NASPO ValuePoint Cooperative Contracts. The central online website is referred to as the NASPO ValuePoint eMarket Center.

The Contractor will have visibility in the eMarket Center through Ordering Instructions. These Ordering Instructions are available at no cost to the Contractor and provided customers information regarding the Contractors website and ordering information.

At a minimum, the Contractor agrees to the following timeline: NASPO ValuePoint eMarket Center Site Admin shall provide a written request to the Contractor to begin Ordering Instruction process. The Contractor shall have thirty (30) days from receipt of written request to work with NASPO ValuePoint to provide any unique information and ordering instructions that the Contractor would like the customer to have.

40. Contract Provisions for Orders Utilizing Federal Funds: Pursuant to Appendix II to 2 Code of Federal Regulations (CFR) Part 200, Contract Provisions for Non-Federal Entity Contracts Under Federal Awards, Orders funded with federal funds may have additional contractual requirements or certifications that must be satisfied at the time the Order is placed or upon delivery. These federal requirements may be proposed by Participating Entities in Participating Addenda and Purchasing Entities for incorporation in Orders placed under this master agreement.

41. Government Support: No support, facility space, materials, special access, personnel or other obligations on behalf of the states or other Participating Entities, other than payment, are required under the Master Agreement.

42. NASPO ValuePoint Summary and Detailed Usage Reports: In addition to other reports that may be required by this solicitation, the Contractor shall provide the following NASPO ValuePoint reports.

a. Summary Sales Data. The Contractor shall submit quarterly sales reports directly to

NASPO ValuePoint using the NASPO ValuePoint Quarterly Sales/Administrative Fee Reporting Tool found at http://calculator.naspovaluepoint.org. Any/all sales made under the contract shall be reported as cumulative totals by state. Even if Contractor experiences zero sales during a calendar quarter, a report is still required. Reports shall be due no later than 30 day following the end of the calendar quarter (as specified in the reporting tool).

b. Detailed Sales Data. Contractor shall also report detailed sales data by: (1) state; (2) entity/customer type, e.g. local government, higher education, K12, non-profit; (3) Purchasing Entity name; (4) Purchasing Entity bill-to and ship-to locations; (4) Purchasing Entity and Contractor Purchase Order identifier/number(s); (5) Purchase Order Type (e.g. sales order, credit, return, upgrade, determined by industry practices); (6) Purchase Order date; (7) and line item description, including product number if used. The report shall be submitted in any form required by the solicitation. Reports are due on a quarterly basis and must be received by the Lead State and NASPO ValuePoint Cooperative Development Team no later than thirty (30) days after the end of the reporting period. Reports shall be delivered to the Lead State and to the NASPO ValuePoint Cooperative Development Team electronically through a designated portal, email, CD-Rom, flash drive or other method as determined by the Lead State and NASPO ValuePoint. Detailed sales data reports shall include sales information for all sales under Participating Addenda executed under this Master Agreement. The format for the detailed sales data report is in shown in Attachment H.

c. Reportable sales for the summary sales data report and detailed sales data report includes sales to employees for personal use where authorized by the solicitation and the Participating Addendum. Report data for employees should be limited to ONLY the state and entity they are participating under the authority of (state and agency, city, county, school district, etc.) and the amount of sales. No personal identification numbers, e.g. names, addresses, social security numbers or any other numerical identifier, may be submitted with any report.

d. Contractor shall provide the NASPO ValuePoint Cooperative Development Coordinator with an executive summary each quarter that includes, at a minimum, a list of states with an active Participating Addendum, states that Contractor is in negotiations with and any PA roll out or implementation activities and issues. NASPO ValuePoint Cooperative Development Coordinator and Contractor will determine the format and content of the executive summary. The executive summary is due 30 days after the conclusion of each calendar quarter.

e. Timely submission of these reports is a material requirement of the Master Agreement. The recipient of the reports shall have exclusive ownership of the media containing the reports. The Lead State and NASPO ValuePoint shall have a perpetual, irrevocable, non-exclusive, royalty free, transferable right to display, modify, copy, and otherwise use reports, data and information provided under this section.

f. If requested by a Participating Entity, the Contractor must provide detailed sales data

within the Participating State.

43. NASPO ValuePoint Cooperative Program Marketing, Training, and Performance Review:

a. Contractor agrees to work cooperatively with NASPO ValuePoint personnel. Contractor agrees to present plans to NASPO ValuePoint for the education of Contractor's contract administrator(s) and sales/marketing workforce regarding the Master Agreement contract, including the competitive nature of NASPO ValuePoint procurements, the Master agreement and participating addendum process, and the manner in which qualifying entities can participate in the Master Agreement.

b. Contractor agrees, as Participating Addendums become executed, if requested by ValuePoint personnel to provide plans to launch the program within the participating state. Plans will include time frames to launch the agreement and confirmation that the Contractor's website has been updated to properly reflect the contract offer as available in the participating state.

c. Contractor agrees, absent anything to the contrary outlined in a Participating Addendum, to consider customer proposed terms and conditions, as deemed important to the customer, for possible inclusion into the customer agreement. Contractor will ensure that their sales force is aware of this contracting option.

d. Contractor agrees to participate in an annual contract performance review at a location selected by the Lead State and NASPO ValuePoint, which may include a discussion of marketing action plans, target strategies, marketing materials, as well as Contractor reporting and timeliness of payment of administration fees.

e. Contractor acknowledges that the NASPO ValuePoint logos may not be used by Contractor in sales and marketing until a logo use agreement is executed with NASPO ValuePoint.

f. The Lead State expects to evaluate the utilization of the Master Agreement at the annual performance review. Lead State may, in its discretion, terminate the Master Agreement pursuant to section 6 when Contractor utilization does not warrant further administration of the Master Agreement. The Lead State may exercise its right to not renew the Master Agreement if vendor fails to record or report revenue for three consecutive quarters, upon 60-calendar day written notice to the Contractor. This subsection does not limit the discretionary right of either the Lead State or Contractor to terminate the Master Agreement pursuant to section 7.

g. Contractor agrees, within 30 days of their effective date, to notify the Lead State and NASPO ValuePoint of any contractual most-favored-customer provisions in third-part contracts or agreements that may affect the promotion of this Master Agreements or whose terms provide for adjustments to future rates or pricing based on rates, pricing in, or Orders from this master agreement. Upon request of the Lead State or NASPO

ValuePoint, Contractor shall provide a copy of any such provisions.

45. NASPO ValuePoint Cloud Offerings Search Tool: In support of the Cloud Offerings Search Tool here: http://www.naspovaluepoint.org/#/contract-details/71/search Contractor shall ensure its Cloud Offerings are accurately reported and updated to the Lead State in the format/template shown in Attachment I.

46. Entire Agreement: This Master Agreement, along with any attachment, contains the entire understanding of the parties hereto with respect to the Master Agreement unless a term is modified in a Participating Addendum with a Participating Entity. No click-through, or other end user terms and conditions or agreements required by the Contractor ("Additional Terms") provided with any Services hereunder shall be binding on Participating Entities or Purchasing Entities, even if use of such Services requires an affirmative "acceptance" of those Additional Terms before access is permitted.

Exhibit 1 to the Master Agreement: Software-as-a-Service

1. Data Ownership: The Purchasing Entity will own all right, title and interest in its data that is related to the Services provided by this Master Agreement. The Contractor shall not access Purchasing Entity user accounts or Purchasing Entity data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Master Agreement, Participating Addendum, SLA, and/or other contract documents, or (4) at the Purchasing Entity's written request.

Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding a Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this Master Agreement.

2. Data Protection: Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized use of Purchasing Entity information at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of Purchasing Entity information and comply with the following conditions:

a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.

b. All data obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.

c. All Personal Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of the Master Agreement.

d. Unless otherwise stipulated, the Contractor shall encrypt all Non-Public Data at rest and in transit. The Purchasing Entity shall identify data it deems as Non-Public Data to the Contractor. The level of protection and encryption for all Non-Public Data shall be identified in the SLA.

e. At no time shall any data or processes — that either belong to or are intended for the use of a Purchasing Entity or its officers, agents or employees — be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the Purchasing Entity.

f. The Contractor shall not use any information collected in connection with the Services issued from this Master Agreement for any purpose other than fulfilling the Services.

3. Data Location: The Contractor shall provide its services to the Purchasing Entity and its end users solely from data centers in the U.S. Storage of Purchasing Entity data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store Purchasing Entity data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access Purchasing Entity data remotely only as required to provide technical support. The Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in a Participating Addendum.

4. Security Incident or Data Breach Notification:

a. Incident Response: Contractor may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing security incidents with the Purchasing Entity should be handled on an urgent as-needed basis, as part of Contractor's communication and mitigation processes as mutually agreed upon, defined by law or contained in the Master Agreement.

b. Security Incident Reporting Requirements: The Contractor shall report a security incident to the Purchasing Entity identified contact immediately as soon as possible or promptly without out reasonable delay, or as defined in the SLA.

c. Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed data breach that affects the security of any purchasing entity's content that is subject to applicable data breach notification law, the Contractor shall (1) as soon as possible or promptly without out reasonable delay notify the Purchasing Entity, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner.

5. Personal Data Breach Responsibilities: This section only applies when a Data Breach occurs with respect to Personal Data within the possession or control of the Contractor.

a. The Contractor, unless stipulated otherwise, shall immediately notify the appropriate Purchasing Entity identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.

b. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it has confirmed that there is, or reasonably believes that there has been a Data Breach. The Contractor shall (1) cooperate with the Purchasing Entity as reasonably requested by the Purchasing Entity to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

c. Unless otherwise stipulated, if a data breach is a direct result of Contractor's breach of its contractual obligation to encrypt personal data or otherwise prevent its release as reasonably determined by the Purchasing Entity, the Contractor shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by federal and state laws or as otherwise agreed to; (3) a credit monitoring service required by state (or federal) law or as otherwise agreed to; (4) a website or a toll-free number and call center for affected individuals required by federal and state laws — all not to exceed the average per record per person cost calculated for data breaches in the United States (currently $217 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Contractor based on root cause.

6. Notification of Legal Requests: The Contractor shall contact the Purchasing Entity upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the Purchasing Entity's data under the Master Agreement, or which in any way might reasonably require access to the data of the Purchasing Entity. The Contractor shall not respond to subpoenas, service of process and other legal requests related to the Purchasing Entity without first notifying and obtaining the approval of the Purchasing Entity, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

a. In the event of a termination of the Master Agreement or applicable Participating Addendum, the Contractor shall implement an orderly return of purchasing entity's data in a CSV or another mutually agreeable format at a time agreed to by the parties or allow the Purchasing Entity to extract it's data and the subsequent secure disposal of purchasing entity's data.

b. During any period of service suspension, the Contractor shall not take any action to intentionally erase or otherwise dispose of any of the Purchasing Entity's data.

c. In the event of termination of any services or agreement in entirety, the Contractor shall not take any action to intentionally erase purchasing entity's data for a period of:

- 10 days after the effective date of termination, if the termination is in accordance with the contract period
- 30 days after the effective date of termination, if the termination is for convenience
- 60 days after the effective date of termination, if the termination is for cause

After such period, the Contractor shall have no obligation to maintain or provide any purchasing entity's data and shall thereafter, unless legally prohibited, delete all purchasing entity's data in its systems or otherwise in its possession or under its control.

d. The purchasing entity shall be entitled to any post termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of an SLA.

e. Upon termination of the Services or the Agreement in its entirety, Contractor shall securely dispose of all Purchasing Entity's data in all of its forms, such as disk, CD/ DVD, backup tape and paper, unless stipulated otherwise by the Purchasing Entity. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the Purchasing Entity.

8. Background Checks: Upon the request of the Purchasing Entity, the Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Master Agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Purchasing Entity's information among the Contractor's employees and agents. If any of the stated personnel providing services under a Participating Addendum is not acceptable to the Purchasing Entity in its sole opinion as a result of the background or criminal history investigation, the Purchasing Entity, in its' sole option shall have the right to either (1) request immediate replacement of the person, or (2) immediately terminate the Participating Addendum and any related service agreement.

9. Access to Security Logs and Reports: The Contractor shall provide reports on a schedule specified in the SLA to the Purchasing Entity in a format as specified in the SLA agreed to by both the Contractor and the Purchasing Entity. Reports shall include latency statistics, user access, user access IP address, user access history and security logs for all public jurisdiction files related to this Master Agreement and applicable Participating Addendum.

10. Contract Audit: The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement terms. The Purchasing Entity may perform this audit or contract with a third party at its discretion and at the Purchasing Entity's expense.

11. Data Center Audit: The Contractor shall perform an independent audit of its data centers at least annually at its expense, and provide an unredacted version of the audit report upon request to a Purchasing Entity. The Contractor may remove its proprietary information from the unredacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

12. Change Control and Advance Notice: The Contractor shall give a minimum forty eight (48) hour advance notice (or as determined by a Purchasing Entity and included in the SLA) to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

Contractor will make updates and upgrades available to Purchasing Entity at no additional costs when Contractor makes such updates and upgrades generally available to its users.

No update, upgrade or other charge to the Service may decrease the Service's functionality, adversely affect Purchasing Entity's use of or access to the Service, or increase the cost of the Service to the Purchasing Entity.

Contractor will notify the Purchasing Entity at least sixty (60) days in advance prior to any major update or upgrade.

13. Security: As requested by a Purchasing Entity, the Contractor shall disclose its non-proprietary system security plans (SSP) or security processes and technical limitations to the Purchasing Entity such that adequate protection and flexibility can be attained between the Purchasing Entity and the Contractor. For example: virus checking and port sniffing — the Purchasing Entity and the Contractor shall understand each other's roles and responsibilities.

14. Non-disclosure and Separation of Duties: The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of Purchasing Entity data to that which is absolutely necessary to perform job duties.

15. Import and Export of Data: The Purchasing Entity shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor at any time during the term of Contractor's contract with the Purchasing Entity. This includes the ability for the Purchasing Entity to import or export data to/from other Contractors. Contractor shall specify if Purchasing Entity is required to provide its' own tools for this purpose, including the optional purchase of Contractors tools if Contractors applications are not able to provide this functionality directly.

16. Responsibilities and Uptime Guarantee: The Contractor shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the Contractor. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.

17. Subcontractor Disclosure: Contractor shall identify all of its strategic business partners related to services provided under this Master Agreement, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Contractor, and who shall be involved in any application development and/or operations.

18. Right to Remove Individuals: The Purchasing Entity shall have the right at any time to require that the Contractor remove from interaction with Purchasing Entity any Contractor representative who the Purchasing Entity believes is detrimental to its working relationship with the Contractor. The Purchasing Entity shall provide the Contractor with notice of its determination, and the reasons it requests the removal. If the Purchasing Entity signifies that a potential security violation exists with respect to the request, the Contractor shall immediately remove such individual. The Contractor shall not assign the

person to any aspect of the Master Agreement or future work orders without the Purchasing Entity's consent.

19. Business Continuity and Disaster Recovery: The Contractor shall provide a business continuity and disaster recovery plan upon request and ensure that the Purchasing Entity's recovery time objective (RTO) of XXX hours/days is met. (XXX hour/days shall be provided to Contractor by the Purchasing Entity.) Contractor must work with the Purchasing Entity to perform an annual Disaster Recovery test and take action to correct any issues detected during the test in a time frame mutually agreed between the Contractor and the Purchasing Entity.

20. Compliance with Accessibility Standards: The Contractor shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973, or any other state laws or administrative regulations identified by the Participating Entity.

21. Web Services: The Contractor shall use Web services exclusively to interface with the Purchasing Entity's data in near real time.

22. Encryption of Data at Rest: The Contractor shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Personal Data, unless the Purchasing Entity approves in writing for the storage of Personal Data on a Contractor portable device in order to accomplish work as defined in the statement of work.

23. Subscription Terms: Contractor grants to a Purchasing Entity a license to: (i) access and use the Service for its business purposes; (ii) for SaaS, use underlying software as embodied or used in the Service; and (iii) view, copy, upload and download (where applicable), and use Contractor's documentation.

No Contractor terms, including standard click through license or website terms or use of privacy policy, shall apply to Purchasing Entities unless such terms are included in this Master Agreement.

Exhibit 2 to the Master Agreement: Platform-as-a-Service

1. Data Ownership: The Purchasing Entity will own all right, title and interest in its data that is related to the Services provided by this Master Agreement. The Contractor shall not access Purchasing Entity user accounts or Purchasing Entity data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Master Agreement, Participating Addendum, SLA, and/or other contract documents, or (4) at the Purchasing Entity's written request.

Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding a Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this Master Agreement.

2. Data Protection: Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized use of Purchasing Entity information at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of Purchasing Entity information and comply with the following conditions:

a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.

b. All data obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.

c. All Personal Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of the Master Agreement.

d. Unless otherwise stipulated, the Contractor shall encrypt all Non-Public Data at rest and in transit. The Purchasing Entity shall identify data it deems as Non-Public Data to the Contractor. The level of protection and encryption for all Non-Public Data shall be identified in the SLA.

e. At no time shall any data or processes — that either belong to or are intended for the use of a Purchasing Entity or its officers, agents or employees — be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the Purchasing Entity.

f. The Contractor shall not use any information collected in connection with the Services issued from this Master Agreement for any purpose other than fulfilling the Services.

3. Data Location: The Contractor shall provide its services to the Purchasing Entity and its end users solely from data centers in the U.S. Storage of Purchasing Entity data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store Purchasing Entity data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access Purchasing Entity data remotely only as required to provide technical support. The Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in a Participating Addendum.

4. Security Incident or Data Breach Notification: The Contractor shall inform the Purchasing Entity of any security incident or data breach within the possession and control of the Contractor and related to the service provided under the Master Agreement, Participating Addendum, or SLA. Such notice shall include, to the best of Contractor's knowledge at that time, the persons affected, their identities, and the Confidential Information and Data disclosed, or shall include if this information is unknown.

a. Incident Response: The Contractor may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the Master Agreement, Participating Addendum, or SLA. Discussing security incidents with the Purchasing Entity should be handled on an urgent as-needed basis, as part of Contractor's communication and mitigation processes as mutually agreed, defined by law or contained in the Master Agreement, Participating Addendum, or SLA.

b. Security Incident Reporting Requirements: Unless otherwise stipulated, the Contractor shall immediately report a security incident related to its service under the Master Agreement, Participating Addendum, or SLA to the appropriate Purchasing Entity.

c. Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed data breach that affects the security of any Purchasing Entity data that is subject to applicable data breach notification law, the Contractor shall (1) promptly notify the appropriate Purchasing Entity within 24 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner

5. Breach Responsibilities: This section only applies when a Data Breach occurs with respect to Personal Data within the possession or control of the Contractor.

a. The Contractor, unless stipulated otherwise, shall immediately notify the appropriate Purchasing Entity identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.

b. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it has confirmed that there is, or reasonably believes that there has been a data breach. The Contractor shall (1) cooperate with the Purchasing Entity as reasonably

requested by the Purchasing Entity to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

c. Unless otherwise stipulated, if a Data Breach is a direct result of Contractor's breach of its contractual obligation to encrypt Personal Data or otherwise prevent its release, the Contractor shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by federal and state laws or as otherwise agreed to; (3) a credit monitoring service required by state (or federal) law or as otherwise agreed to; (4) a website or a toll-free number and call center for affected individuals required by federal and state laws — all not to exceed the average per record per person cost calculated for data breaches in the United States (currently $217 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Contractor based on root cause.

6. Notification of Legal Requests: The Contractor shall contact the Purchasing Entity upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the Purchasing Entity's data under the Master Agreement, or which in any way might reasonably require access to the data of the Purchasing Entity. The Contractor shall not respond to subpoenas, service of process and other legal requests related to the Purchasing Entity without first notifying and obtaining the approval of the Purchasing Entity, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

a. In the event of an early termination of the Master Agreement, Participating or SLA, Contractor shall allow for the Purchasing Entity to retrieve its digital content and provide for the subsequent secure disposal of the Purchasing Entity's digital content.

b. During any period of service suspension, the Contractor shall not take any action to intentionally erase or otherwise dispose of any of the Purchasing Entity's data.

c. In the event of early termination of any Services or agreement in entirety, the Contractor shall not take any action to intentionally erase any Purchasing Entity's data for a period of 1) 45 days after the effective date of termination, if the termination is for convenience; or 2) 60 days after the effective date of termination, if the termination is for cause. After such day period, the Contractor shall have no obligation to maintain or provide any Purchasing Entity data and shall thereafter, unless legally prohibited, delete all Purchasing Entity data in its systems or otherwise in its possession or under its control. In the event of either termination for cause, the Contractor will impose no fees for access and retrieval of digital content to the Purchasing Entity.

d. The Purchasing Entity shall be entitled to any post termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of an SLA.

e. Upon termination of the Services or the Agreement in its entirety, Contractor shall securely dispose of all Purchasing Entity's data in all of its forms, such as disk, CD/ DVD, backup tape and paper, unless stipulated otherwise by the Purchasing Entity. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the Purchasing Entity.

8. Background Checks:

a. Upon the request of the Purchasing Entity, the Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Master Agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Purchasing Entity's information among the Contractor's employees and agents.

b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

c. If any of the stated personnel providing services under a Participating Addendum is not acceptable to the Purchasing Entity in its sole opinion as a result of the background or criminal history investigation, the Purchasing Entity, in its' sole option shall have the right to either (1) request immediate replacement of the person, or (2) immediately terminate the Participating Addendum and any related service agreement.

9. Access to Security Logs and Reports:

a. The Contractor shall provide reports on a schedule specified in the SLA to the Purchasing Entity in a format as specified in the SLA and agreed to by both the Contractor and the Purchasing Entity. Reports will include latency statistics, user access, user access IP address, user access history and security logs for all Purchasing Entity files related to the Master Agreement, Participating Addendum, or SLA.

b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

10. Contract Audit: The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement terms. The Purchasing Entity may perform this audit or contract with a third party at its discretion and at the Purchasing Entity's expense.

11. Data Center Audit: The Contractor shall perform an independent audit of its data centers at least annually at its expense, and provide an unredacted version of the audit report upon request to a Purchasing Entity. The Contractor may remove its proprietary information from the unredacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

12. Change Control and Advance Notice: The Contractor shall give a minimum forty eight (48) hour advance notice (or as determined by a Purchasing Entity and included in the SLA) to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

Contractor will make updates and upgrades available to Purchasing Entity at no additional costs when Contractor makes such updates and upgrades generally available to its users.

No update, upgrade or other charge to the Service may decrease the Service's functionality, adversely affect Purchasing Entity's use of or access to the Service, or increase the cost of the Service to the Purchasing Entity.

Contractor will notify the Purchasing Entity at least sixty (60) days in advance prior to any major update or upgrade.

13. Security: As requested by a Purchasing Entity, the Contractor shall disclose its non-proprietary system security plans (SSP) or security processes and technical limitations to the Purchasing Entity such that adequate protection and flexibility can be attained between the Purchasing Entity and the Contractor. For example: virus checking and port sniffing — the Purchasing Entity and the Contractor shall understand each other's roles and responsibilities.

14. Non-disclosure and Separation of Duties: The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of Purchasing Entity data to that which is absolutely necessary to perform job duties.

15. Import and Export of Data: The Purchasing Entity shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor at any time during the term of Contractor's contract with the Purchasing Entity. This includes the ability for the Purchasing Entity to import or export data to/from other Contractors. Contractor shall specify if Purchasing Entity is required to provide its' own tools for this purpose, including the optional purchase of Contractors tools if Contractors applications are not able to provide this functionality directly.

16. Responsibilities and Uptime Guarantee: The Contractor shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the Contractor. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.

17. Subcontractor Disclosure: Contractor shall identify all of its strategic business partners related to services provided under this Master Agreement, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Contractor, and who shall be involved in any application development and/or operations.

18. Business Continuity and Disaster Recovery: The Contractor shall provide a business continuity and disaster recovery plan upon request and ensure that the Purchasing Entity's recovery time objective (RTO) of XXX hours/days is met. (XXX hour/days shall be provided to Contractor by the Purchasing Entity.) Contractor must work with the Purchasing Entity to perform an annual Disaster Recovery test and take action to correct any issues detected during the test in a time frame mutually agreed between the Contractor and the Purchasing Entity.

19. Compliance with Accessibility Standards: The Contractor shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973 or any other state laws or administrative regulations identified by the Participating Entity..

20. Web Services: The Contractor shall use Web services exclusively to interface with the Purchasing Entity's data in near real time.

21. Encryption of Data at Rest: The Contractor shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Personal Data as identified in the SLA, unless the Contractor presents a justifiable position that is approved by the Purchasing Entity that Personal Data, is required to be stored on a Contractor portable device in order to accomplish work as defined in the scope of work.

22. Subscription Terms: Contractor grants to a Purchasing Entity a license to: (i) access and use the Service for its business purposes; (ii) for PaaS, use underlying software as embodied or used in the Service; and (iii) view, copy, upload and download (where applicable), and use Contractor's documentation.

No Contractor terms, including standard click through license or website terms or use of privacy policy, shall apply to Purchasing Entities unless such terms are included in this Master Agreement.

Attachment B – Scope of Services Awarded to Contractor

1.1 Awarded Service Model(s).

Contractor is awarded the following Service Model:

- Platform as a Service (PaaS)
- Software as a Service (SaaS)

1.2 Risk Categorization.*

Contractor's offered solutions offer the ability to store and secure data under the following risk categories:

Service Model	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered
PaaS	X	X	X	Community, Hybrid, Private, Public
SaaS	X	X	X	Community, Hybrid, Private, Public

*Contractor may add additional OEM solutions during the life of the contract.

2.1 Deployment Models.

Contractor may provide cloud based services through the following deployment methods:

- **Private cloud.** The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
- **Community cloud.** The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
- **Public cloud.** The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
- **Hybrid cloud.** The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)

Attachment C - Pricing Discounts and Schedule

Contractor: Armedia, LLC

Pricing Notes

1. % discounts are based on minimum discounts off Contractor's commercially published pricelists versus fixed pricing. Nonetheless, Orders will be fixed-price or fixed-rate and not cost reimbursable contracts. Contractor has the ability to update and refresh its respective price catalog, as long as the agreed-upon discounts are fixed.
2. Minimum guaranteed contract discounts do not preclude an Offeror and/or its authorized resellers from providing deeper or additional, incremental discounts at their sole discretion.
3. Purchasing entities shall benefit from any promotional pricing offered by Contractor to similar customers. Promotional pricing shall not be cause for a permanent price change.
4. Contractor's price catalog include the price structures of the cloud service models, value added services (i.e., Maintenance Services, Professional Services, Etc.), and deployment models that it intends to provide including the types of data it is able to hold under each model. Pricing shall all-inclusive of infrastructure and software costs and management of infrastructure, network, OS, and software.
5. Contractor provides tiered pricing to accompany its named user licensing model, therefore, as user count reaches tier thresholds, unit price decreases.

Cloud Service Model: Platform as a Service (PaaS)

Description	Discount
Armedia-ADF	5.00%
Armedia-ADF-100	10.00%
Armedia-ADF-500	25.00%
Armedia-ADF-1000	35.00%
Armedia-ADF-5000	45.00%
Armedia-ACC-100	5.00%
Armedia-ACC-300	10.00%
Armedia-ACC-1000	15.00%
Average PaaS OEM Discount Off	**18.75%**

Cloud Service Model: Software as a Service (SaaS)

Description	Discount
ArkCase SaaS (less than 99 users)	5.00%
ArkCase SaaS 100 (100 users to 499 users)	10.00%
ArkCase SaaS 500 (500 users to 999 users)	25.00%
ArkCase SaaS 1000 (1000 users to 4999 users)	35.00%
ArkCase SaaS 5000 (more than 5000 users)	45.00%
Armedia Business Solution Add-on for ArkCase	5.00%
Armedia Business Solution Add-on for ArkCase 100	10.00%
Armedia Business Solution Add-on for ArkCase 500	25.00%
Armedia Business Solution Add-on for ArkCase 1000	35.00%
Armedia Business Solution Add-on for ArkCase 5000	45.00%
Average SaaS OEM Discount Off	**28.75%**

Additional Value Added Services

		Onsite Hourly Rate		Remote Hourly Rate	
Item Description		**NVP Price**	**Catalog Price**	**NVP Price**	**Catalog Price**
Maintenance Services		$104.28	$107.51	$109.50	$112.89
Professional Services					
	Deployment Services	$124.75	$128.61	$130.99	$135.04
	Integration Services	$111.73	$115.19	$117.32	$120.95
	Consulting/Advisory Services	$178.19	$183.70	$187.10	$192.89
	Architectural Design Services	$156.41	$161.25	$164.23	$169.31
	Statement of Work Services	$118.50	$122.17	$124.43	$128.28
Partner Services		$137.74	$142.00	$144.63	$149.10
Training Deployment Services		$98.39	$101.43	$103.31	$106.50
Program Management Services		$147.59	$152.15	$154.96	$159.76
Analysis Services		$137.74	$142.00	$144.63	$149.10
Testing and Quality Assurance Services		$76.32	$78.68	$80.14	$82.61
Help Desk Services		$40.98	$42.25	$43.03	$44.36
Document Capture Services		$33.28	$34.31	$34.94	$36.03
Migration Services		$118.50	$122.17	$124.43	$128.28

Deliverable Rates

Attachment C - Pricing Discounts and Schedule

Contractor: Armedia, LLC

	NVP Price	Catalog Price
Annual Support Package 100 (pre-paid annual bucket of	$12,217.95	$12,861.00
Annual Support Package 500 (pre-paid annual bucket of	$59,803.65	$64,305.00
Annual Support Package 1000 (pre-paid annual bucket of	$117,035.10	$128,610.00
Annual Support Package 5000 (pre-paid annual bucket of	$565,884.00	$643,050.00
Monthly 24x7 Remote Help Desk package (per person)	$11,400.00	$12,000.00
[Insert additional value added services as necessary]		

The State of Utah
Division of Purchasing

In conjunction with

Response to:

Utah Solicitation Number SK18008

NASPO ValuePoint

NASPO ValuePoint Master Agreement for Cloud Solutions
Technical Response Software as a Service

Submitted by:
Armedia, LLC
8221 Old Courthouse Road, Suite 300
Vienna, VA 22182
www.armedia.com
Mr. James Bailey
President
703-272-3270 (O)
703-935-3030 (F)
james.bailey@armedia.com

CMMI Level 3 Appraised
Veteran Owned Small Business (VOSB)
TIN - 30-0067329
DUNS – 1330
CAGE/NCAGE Code – 3HAW7
GSA IT70 - GS35F0891P

Submitted to:
Mr. Solomon Kingston
State Contract Analyst
State of Utah, Division of Purchasing
skingston@utah.gov
(801)538 - 3228

Table of Contents

6 TECHNICAL RESPONSE

Armedia is an Amazon Web Service (AWS) Consulting partner specializing in building SaaS solutions using cloud technologies and infrastructure. We specialize in building cost-effective, secure and scalable cloud-based solutions in the areas of content management, data analytics, system usage and behavior analysis, machine learning and business process automations.

With our staff of certified cloud engineers and solution developers, Armedia is well suited to support NASPO's Purchasing Entities with their cloud migration and cloud adoptions through SaaS and PaaS implementations.

Armedia offers its business process automation tool – ArkCase (depicted in Figure 1) – as a SaaS offering to NASPO and all its Purchasing Entities. Besides this, Armedia also offers

- Armedia Development Framework (ADF) for extending ArkCase and developing custom solutions using ArkCase and
- Armedia Content Cloud (ACC) – a fully configured AWS setup for deploying ArkCase SaaS and ADF based custom applications

ArkCase is a fully integrated system for case management and business process automation that provides content management, content authoring, version control, collaboration, workflow, data and metadata enhancement, editing, publishing, statistical reporting, and search and retrieval capabilities along with a knowledge management component that makes it ideally capable of supporting NASPO in the key areas of information research, data analysis, content management, compliance management, case management and business process automation.

ArkCase is used as a SaaS model for the following functional sub-categories:

- Analytics – Business Intelligence
- Customer Relationship Management
- Collaboration
- Data Management
- E-Discovery
- Electronics Records Management
- Licensing and Registration Systems
- Workflow and Electronic Signature

At its core, ArkCase is a business process automation tool that provides core services that include:

- Document/Information Management
- Records Management
- Case Management
- Task Management
- Workflow Configuration and Management
- Security and Access Control
- Database Management
- User Account and Profile Management
- Auditing and Reporting
- Contact Management

- Communications, Alerts and Notifications Management

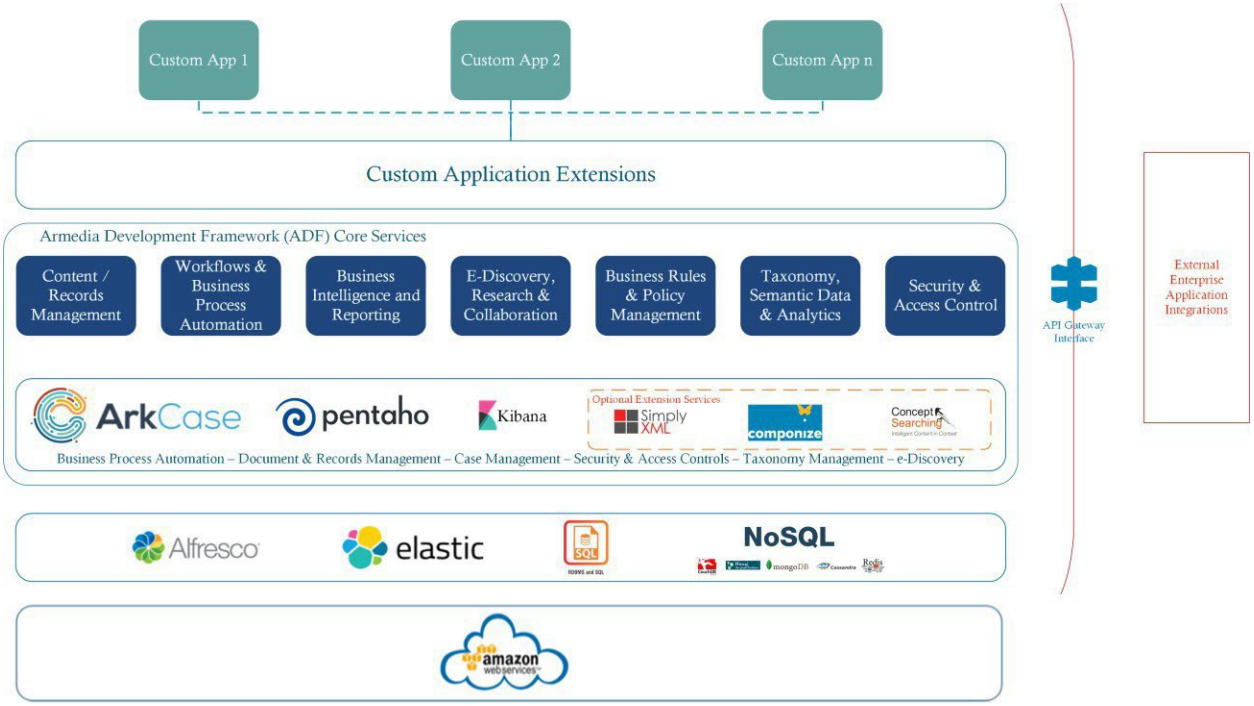


Figure 1 – ArkCase – Armedia's SaaS offering for business process automation and case management

Out-of-the-box, the Purchasing Entity can use ArkCase for:

- Case Management
- Compliance Management
- Complaints Management
- Licensing Process Management
- Task Management
- FOIA Request Processing

ArkCase as SaaS is available to the Purchasing Entities under the following configurations:

- Basic ArkCase – a basic business process automation platform that can be configured and used for case management, compliance management, complaints management and task management.
- ArkCase Legal – ships with the basic features plus specific business process workflows for legal case management, evidence management and digital asset management with DoD 5015.2 complaint records management.
- FOIA request processing – ships with business process workflows for processing and tracking Freedom of Information Act (FOIA) request.

The Purchasing Entity has multiple service options for ArkCase:

- Self-managed service for ArkCase cloud deployment (SaaS) – an out-of-the-box, Amazon Machine Image (AMI) based instantiation of ArkCase platform. The Purchasing Entity can setup ArkCase AMIs and configure the ArkCase Case Management and/or FOIA processing instances for its customer through the ArkCase admin console that allows configuration of the user interface as well user groups and access control policies. The Purchasing Entity does receive direct access to the underlying cloud infrastructure

including network, servers, operating systems, storage etc., which is provisioned by the ArkCase setup.

The Purchasing Entity will have access to ArkCase User and ArkCase Administrator guides. Additionally, the Purchasing Entity will have access to tiered service contracts through Armedia for ArkCase support available under varying SLA terms and pricing.

While ArkCase provides role-based access controls and user groups, configuring the access control policies would be the responsibility of the Purchasing Entity based on the instructions in the User and Administrator guides. The data ownership will reside with either the Purchasing Entity and/or its customer based on the service agreement between the Purchasing Entity with their customers. Though ArkCase provides data security by encrypting the data at rest and in transit and has watchers looking out for data breaches, the resolution of breach in the event of a self-managed SaaS implementation is the responsibility of the Purchasing Entity.

- Armedia's white glove managed service for ArkCase deployment (SaaS/PaaS) – a customized ArkCase deployment for any business process automation that can cover case, complaints, compliance, license processing, task management etc. Armedia provides customized physical infrastructure setups that include high-availability and high-scalability setup depicted in Figure 2. This is a fully managed ArkCase service that is managed by Armedia on behalf of the Purchasing Entity. Armedia manages the physical cloud infrastructure setup along with its security and scalability by extending the AWS SLAs. Armedia will resolve any potential data breaches under fully managed SaaS service implementation according to an agreed upon breach resolution policy between Armedia and the Purchasing Entity.

Self-Managed ArkCase SaaS	Fully-Managed ArkCase SaaS
Purchasing Entity sets up AMI instances of ArkCase for its customers.	Armedia sets up the cloud infrastructure for ArkCase on behalf of the Purchasing Entity.
The cloud resources are allocated based on a pre-defined optimum cloud configuration for ArkCase.	The cloud resources can be customized to suit the requirements of the Purchasing Entity and its clients.
Purchasing Entity and its customer own and manage the data based on the agreement between the Purchasing Entity and its customer	Armedia manages the data that is owned by the Purchasing Entity and/or its customer – Armedia does not get access to the data that is protected by data encryption protocols and controlled by the Purchasing Entity and its customer.
Basic Armedia support for ArkCase is included. Additional support options are available to the Purchasing Entity.	Full support is included for the duration of the contract.

In both scenarios, the ArkCase deployment is compliant with FedRAMP moderate security controls. The ownership of the data is always retained by the Purchasing Entity and is always stored on encrypted storage devices.

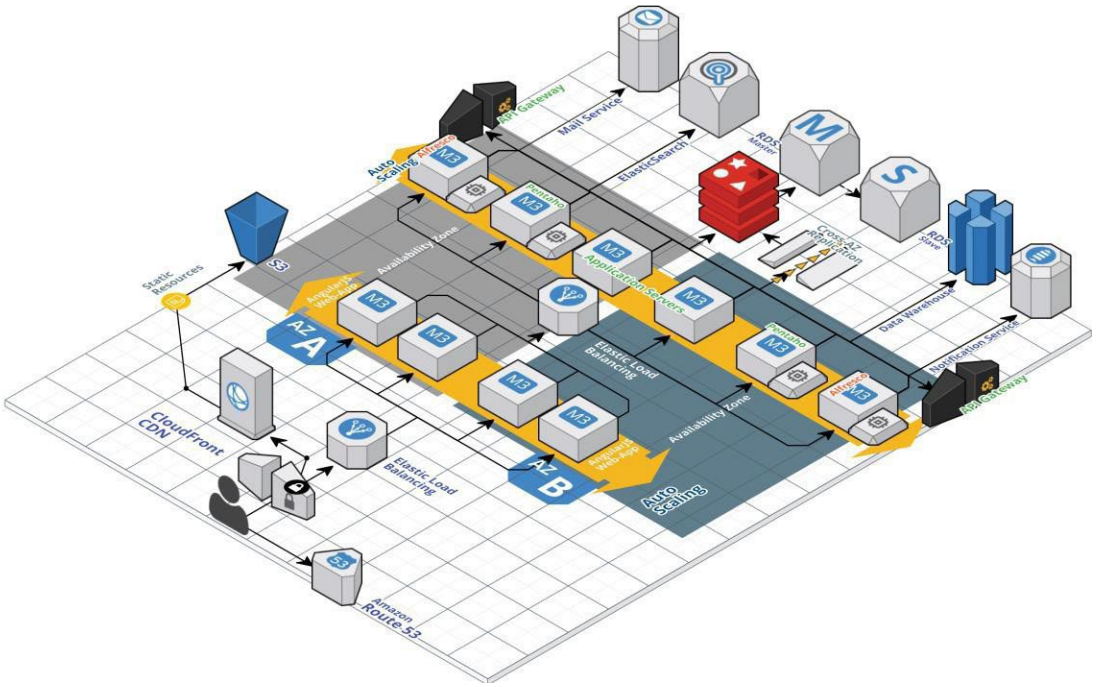


Figure 2 - ArkCase architecture on cloud – high-availability, high-scalability

Figure 2 shows ArkCase could setup using AWS auto-scaling spread across multiple availability zones.

Use of AWS auto-scaling ensures scalability of the ArkCase SaaS while the use of multiple availability zones ensures high availability of the ArkCase SaaS

6.1 Technical Requirements

6.1.1 NIST

8.1.1 For the purposes of the RFP, meeting the NIST essential characteristics is a primary concern. As such, describe how your proposed solution(s) meet the characteristics defined in NIST Special Publication 800-145.

Armedia's PaaS and SaaS offerings are designed and operated as cloud-based services, as defined in NIST Special Publication 800-145 - see the response to sections 8.1.2 and 8.1.3. In addition, Armedia follows applicable information security controls for a Moderate impact system from NIST Special Publication 800-53 as a configuration, architectural, and operational baseline.

The National Institute of Standards and Technology (NIST) 800-53 security controls are generally applicable to Federal Information Systems. These are typically systems that must go through a formal assessment and authorization process to ensure sufficient protection of confidentiality, integrity, and availability of information and information systems, based on the security category and impact level of the system (low, moderate, or high), and a risk determination.

Armedia has standardized on FedRAMP as the common security framework which is based on the NIST 800-53 Rev. 4 security controls, and has extra requirements based on the impact levels for ArkCase as SaaS. Armedia has elected to abide by the Moderate impact level. In order to obtain FedRAMP accreditation, a Third-Party Assessment Organization (3PAO) must be engaged to audit

the System Security Plan (SSP). The 3PAO will review the policies and procedures as well as verify evidence the organization is following the controls and practices. Many of the FedRAMP controls overlap HIPAA's security rules. NIST's 800-66 document the alignment of the NIST 800-53 controls used by FedRAMP and HIPAA's security rules.

Armedia's ArkCase SaaS relies on AWS' NIST-compliant cloud infrastructure services that have been validated by third-party testing performed against the NIST 800-53 Rev. 4 controls plus FedRAMP requirements. AWS has received FedRAMP Authorizations to Operate (ATO) from multiple authorizing agencies for both the AWS GovCloud (US) Region and the AWS US East/West regions.

6.1.2 Requirements of Attachments C & D

8.1.2 As applicable to an Offeror's proposal, Offeror must describe its willingness to comply with, the requirements of Attachments C & D.

Visibility to Purchasing Entities:
Armedia offers ArkCase both as SaaS – where the out-of-the-box case management implementation is available to the purchasing entities under two deployment models described (self-managed and fully-managed), as well as PaaS – where Armedia offers the Armedia Development Framework (ADF) that uses ArkCase for custom application development and deployment.

Primary Focus of the Service:
ArkCase as a service is primarily focused on SaaS model. The ArkCase application can be instantiated by the purchasing entities and configured for any business process automation need.

Purchasing Entity Role:
The Purchasing Entity can instantiate and configure ArkCase for its consumers under the SaaS model thereby providing its customers with Business Process Automation as a Service (BPaaS).

Lowest Level of Configurability:
The lowest level of configurability for an out-of-the-box implementation of ArkCase is as SaaS. The Purchasing Entity can instantiate ArkCase instances for its customers and configure the instance to suit the customer's needs through the intuitive admin interface depicted in *Figure 3 - ArkCase Admin Console*

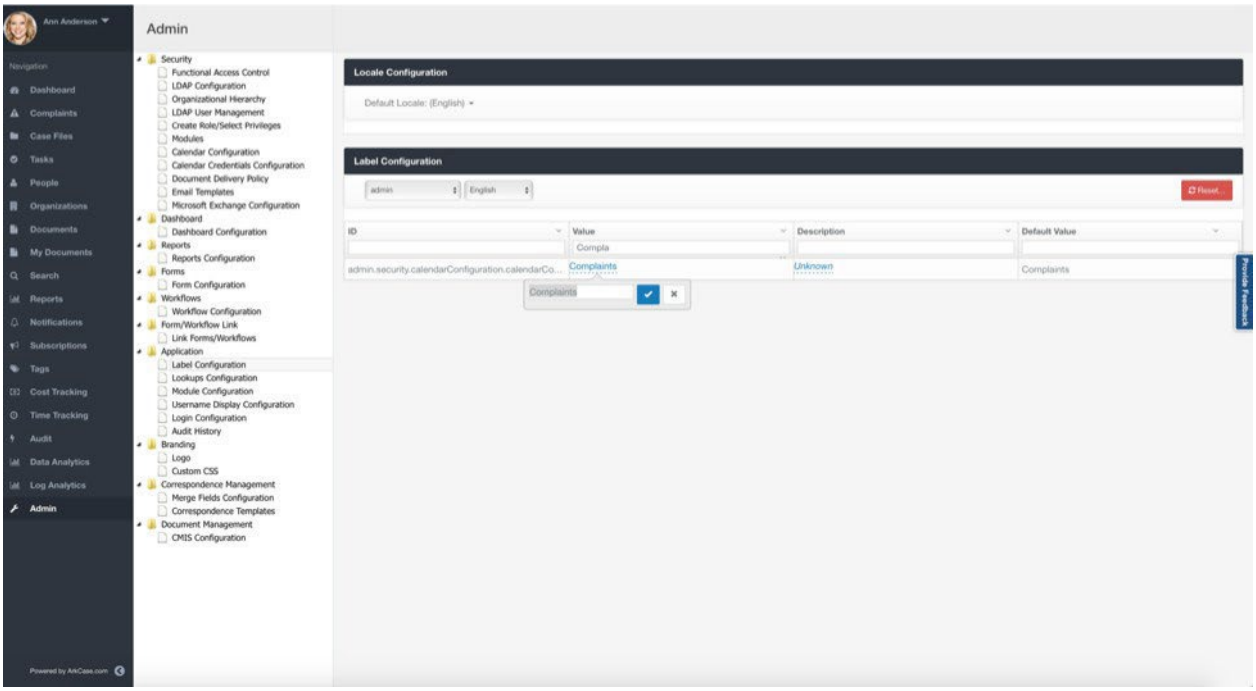


Figure 3 - ArkCase Admin Console

The SaaS setup of ArkCase will configure the cloud infrastructure needed for the platform including network, servers, storage, applications and services.

When Purchasing Entities choose self-managed ArkCase instances, the Purchasing Entity will be responsible to manage the cloud resources that the SaaS setup uses. When using the Armedia managed ArkCase service, Armedia will manage all the cloud resources for the Purchasing Entity. While Armedia manages the cloud resources, data is secure and protected through in-built data protection mechanisms that includes data encryption at rest.

*8.1.3 As applicable to an Offeror's proposal, Offeror must describe how its offerings adhere to the services, definitions, and deployment models identified in the Scope of Services, in **Attachment D**.*

Categorization of Risk

ArkCase is designed to handle Moderate and Low Risk Data with emphasis on data security. ArkCase follows FedRAMP's requirements for a Moderate classification on its operations and uses NIST 800-53 for the baseline security controls. Following NIST's 800-53 controls allows ArkCase to meet HIPAA requirements (see NIST's 800-66 which provides the alignment of NIST 800-53 and HIPAA Security rules). ArkCase uses AWS's EBS encryption to encrypt data at rest and all snapshots created from the volume. Volumes are encrypted using AES-256 by AWS's Key Management Service (KMS). By default, Armedia uses AWS's KMS to create, manage, and rotate keys. An option exists to import existing keys owned by NASPO's Purchasing Entities if required. All data is encrypted in transit using TLS 1.1 or 1.2. This includes communications from the Internet into the entry point of the system, as well as internal communications (web servers to application

AWS Key Management Service provides centralized control over the encryption keys used to protect data. Armedia will work with NASPO's Purchasing Entities to create, import, rotate, disable, delete, define usage policies for, and audit the use of encryption keys used to encrypt data. AWS Key Management Service is integrated with several other AWS services making it

servers, application servers to databases, all directory services, monitoring traffic, etc.).

ArkCase multi-zonal architecture provides additional protection for the data by placing the data behind multiple layers of security through multiple private subnets on AWS VPC. Encrypting the data in transit and at rest further enhances data security.

Service & Models

The NIST definition lists five essential characteristics of cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion, and measured service. The definition is intended to serve as a means for broad comparisons of cloud services and deployment strategies, and to provide a baseline for discussion from what is cloud computing to how to best use cloud computing. The following sections detail how ArkCase SaaS on AWS meets the NIST definition of cloud.

On-demand self-service:

ArkCase is offered as a SaaS available as an on-demand self-service model. The Purchasing Entity can use the one-click setup of ArkCase to deploy the stack on cloud with the appropriate servers, network bandwidth, storage and database services auto-configured for the instantiation. In the self-service mode, the Purchasing Entity will get access to the ArkCase User and ArkCase Administrator guides. Additionally, Armedia offers tiered service contracts for ArkCase that are available to the Purchasing Entity for additional cost based on the desired SLAs.

Armedia also offers a fully managed ArkCase instantiation where Armedia manages all the software and cloud hardware resources on behalf of the Purchasing Entity.

Broad Network Access:

ArkCase user interface is a web application built using AngularJS and responsive UI design templates. This makes ArkCase accessible through heterogeneous thin and thick clients like mobile phones, tablets, laptops and workstations.

In self-service mode, the Purchasing Entity will have access to an admin console that provides a simple way to access the cloud servers, storage, databases and other resources used for ArkCase.

When using Armedia's fully managed ArkCase setup, the cloud resource access is maintained and managed by Armedia's certified cloud engineers.

Resource Pooling:

For consumer data security and data protection, ArkCase currently deploys as separate instantiation for each customer. For each instantiation, the infrastructure resources (e.g., storage, processing, memory and network bandwidth) are auto-assigned and are configured to leverage the auto-scaling ability of the underlying cloud service provider for dynamic assignment and re-assignment as per the consumer demand.

Rapid Elasticity:

ArkCase resources and services are auto-assigned during instantiation and are configured to leverage the elastic load balancing and auto-scaling features of the underlying cloud service

provider. This allows ArkCase to elastically provision and release resources such as processing, memory and network bandwidth, and to scale rapidly commensurate with the consumer demand.

Measured Service:
ArkCase deployed on AWS cloud uses AWS automated monitoring systems to provide a high-level of service performance and availability. Proactive monitoring is available through a variety of online tools both for internal and external use. Systems within AWS are extensively instrumented to monitor key operational metrics. Alarms are configured to notify operations and management personnel when early warning thresholds are crossed on key operational metrics. An on-call schedule is used such that personnel are always available to respond to operational issues. This includes a pager system so alarms are quickly and reliably communicated to operations personnel.

8.1.4 A successful Offeror will have the ability to provide cloud-based services through the following deployment methods:

ArkCase can be deployed on any cloud-based model that includes

- Private Cloud
- Community Cloud
- Public Cloud
- Hybrid-Cloud
- On-Premise

The use of containerized deployment for ArkCase using Kubernetes and Docker allows the platform to be easily deployed to any environment.

6.2 SubContractors

8.2.1 Offerors must explain whether they intend to provide all cloud solutions directly or through the use of Subcontractors.

Armedia is fully qualified to provide all cloud solutions directly without the use of Subcontractors. Our more than eight (8) years of past performance experience demonstrates Armedia's ability to provide these PaaS services without the use of Subcontractors.

8.2.2 Offeror must describe the extent to which it intends to use subcontractors to perform contract requirements.

Armedia does not intend to use subcontractors to perform contract requirements.

8.2.3 If the subcontractor is known, provide the qualifications of the subcontractor to provide the services; if not, describe how you will guarantee selection of a subcontractor that meets the experience requirements of the RFP.

This section is not applicable to Armedia's offer. We do not intend to use subcontractors to perform contract requirements.

6.3 Working with Purchasing Entities

6.3.1 After a Data Breach

8.3.1 Offeror must describe how it will work with Purchasing Entities before, during, and after a Data Breach, as defined in the Attachments and Exhibits. Include information such as:

- *Personnel who will be involved at various stages, include detail on how the Contract Manager in Section 7 will be involved;*
- *Response times;*
- *Processes and timelines;*
- *Methods of communication and assistance; and*
- *Other information vital to understanding the service you provide.*

	Self-Managed ArkCase SaaS	Fully-Managed ArkCase SaaS
Personnel involvement	The Purchasing Entity will be responsible for any remediation. Armedia support will be available based on the purchased support service subscription.	Armedia will be responsible for any remediation in the event of the data breach. The Purchasing Entities and their customers will be notified of any breach occurrence and the remediation steps taken as agreed in the service agreement between Armedia and the Purchasing Entity.
	Armedia's support staff will respond to any requests received from the Purchasing Entity pursuant to the terms of the purchased support levels.	Armedia's support staff will respond to any data breach on a priority basis as soon as it is detected or reported and will notify the concerned parties as per the SLAs.
Response Times	Response times will be determined by the Purchasing Entity. Armedia's response times to the Purchasing Entity will be based on the purchased support contract.	Armedia shall immediately notify (within 24 hours) Purchasing Entity if Armedia becomes aware of any accidental or unauthorized disclosure, access or use of any Personal Information or Confidential Information or a violation of applicable privacy or data protection laws (a "Breach") or if Armedia receives an access request, investigative notice, seizure or complaint from a government or data subject related to Purchasing Entity's Confidential Information (unless such notification is prohibited). Armedia shall use its best efforts to immediately remedy any Breach and prevent any further Breach at its sole expense. In the event of any
Remediation	The remediation process and timelines will be defined by the Purchasing Entity	

	Self-Managed ArkCase SaaS	Fully-Managed ArkCase SaaS
		such Breach, Armedia shall immediately coordinate with Purchasing Entity regarding the response to, and investigation of, the Breach, and cooperate fully with Purchasing Entity, including facilitating interviews with employees and other parties, making available all relevant records, logs, files, data reporting and other materials, and providing Purchasing Entity with physical access to the facilities affected. In the event of a Breach of Personal Information in Armedia's possession or otherwise caused by or related to Armedia's acts or omissions, and without limiting Purchasing Entity's other rights and remedies, Armedia will pay all reasonable costs and expenses of any disclosures and notification required by applicable law or as otherwise determined as appropriate in Purchasing Entity's reasonable discretion, monitoring and reporting on the impacted individuals' or entities' credit records if determined in Purchasing Entity's reasonable discretion as reasonable to protect such individuals, and all other costs incurred by Purchasing Entity in responding to and mitigating damages caused by such Breach.
Communication	The methods of communication will be defined by the Purchasing Entity	Armedia will notify the Purchasing Entity and their affected Customers via emails of any data breach detected. The remediation and the steps taken will also be communicated through emails.

	Self-Managed ArkCase SaaS	Fully-Managed ArkCase SaaS
		Armedia also recommends setting up change control boards comprising of Armedia PM, Purchasing Entity and its Customers' staff and having periodic CCB meetings where the breaches and the remediation can be communicated

Armedia will work with Purchasing Entity to modify the Figure 4 - Armedia Standard Language to Govern Data and Data Breaches. Armedia understands the trust that comes with managing a customer's data and we will use the best practices that we have employed with supporting our Top-Secret clients for over 16 years to include FBI, Joint Staff, and DIA.

5.3.1.1 Use. Confidential Information of the other party will be used solely as necessary to fulfill obligations under this Agreement and for no other purpose whatsoever. Confidential Information of the other may be disclosed internally on a "need to know" basis and shall not be made available to any third party except as specifically authorized by the disclosing party in writing. The receiving party agrees that nothing in this Agreement grants to the receiving party any license, right, title, or interest in or to the Confidential Information, except as expressly set forth herein. The parties agree to protect the other's Confidential Information using the same degree of care they use to protect their own confidential information of a like nature, but never less than ordinary care. Within thirty (30) days of the termination of this Agreement, or promptly upon the disclosing party's written request, the receiving party (i) will cease using and delete/destroy or return the disclosing party's Confidential Information and (ii) provide written confirmation to disclosing party upon request.

5.2 Exclusions/Exceptions. Confidential information does not include information that: (i) was known to a receiving party without restriction before receipt from the disclosing party; (ii) is publicly available through no fault of the receiving party; (iii) is rightfully received by the receiving party from a third party without a duty of confidentiality; or, (iv) is independently developed by the receiving party without reference to any Confidential Information. A receiving party may disclose Confidential Information as necessary to comply with a valid judicial or other governmental order, provided that the receiving party shall: (i) give the disclosing party reasonable written notice, to the extent permitted by law, and an opportunity to object prior to such disclosure; (ii) seek confidential treatment similar to the terms provided in this Agreement of such Confidential Information; and, (iii) comply with any applicable protective order or its equivalent.

5.3 Remedies. In the event of actual or threatened breach of the foregoing Confidential Information provisions resulting in immediate, substantial and irreparable harm to the disclosing party and the disclosing party will have no adequate remedy at law, the disclosing party may seek immediate injunctive and other equitable relief, without bond and without the necessity of showing actual money damages.

5.4 Data Security; Personal Information.

a. Personal Information. Offeror hereby acknowledges that during the performance of this Agreement, Offeror may have access to, collect, receive, transmit and/or store information that identifies or could identify (or potentially be matched with) Purchasing Entity's clients, consumers, employees, contractors or business partners, including but not limited to names, addresses, phone numbers, email addresses, job titles, dates of birth, user names, passwords, IP addresses, locations, Social Security or other identification numbers, health information, biometric data, financial account numbers or credit card information (all hereinafter, "Personal Information"). To the extent that Offeror uses subcontractors that may have access to, collect, receive, transmit or store Personal Information, Offeror will notify Purchasing Entity of such subcontractors and ensure that such subcontractors execute written agreements agreeing to bound by and comply with the terms set forth in this Section.

b. Standard of Care. The Personal Information may only be used by Offeror for the purpose of providing Services under this Agreement and any other statements of work and in accordance with Purchasing Entity's instructions. Offeror will collect, store, transfer, dispose, disclose and use all Personal Information using the highest standard of care to ensure the integrity of such data and in compliance with all applicable federal, state and international privacy and data security laws, regulations and directives. In addition, Offeror shall: (i) use its best efforts to maintain administrative, technical, and physical safeguards that are no less vigorous than industry best practices to ensure the security and confidentiality of the Personal Information, protect against any anticipated threats or hazards to the security or integrity of the Personal Information, and protect against unauthorized access, use, or alteration of any Personal Information; (ii) not disclose any Personal Information to any person unless Purchasing Entity has given its prior written consent to such disclosure; and (iii) continually perform self-checks, including, but not limited to scanning for viruses and other contaminants to ensure that such software products have been found to be free of contaminants and viruses identifiable by such scans, and testing against publicized threats, data infiltrations and breaches to ensure the security and confidentiality of the Personal Information, in order to protect against unauthorized access, use, or alteration of the Personal Information. Upon termination of this Agreement for any reason, or upon request by Purchasing Entity, Offeror shall promptly return to Purchasing Entity all Personal Information, or at Purchasing Entity' request destroy all Personal Information and provide written certification to Purchasing Entity of such destruction.

c. Information Security. Offeror agrees that it will use its best efforts to implement administrative, technical, and physical safeguards that are no less vigorous that industry best practices to insure the security and confidentiality of Personal information and Confidential Information, protect against any anticipated threats or hazards to the confidentiality, availability or integrity of Personal Information and Confidential Information, and protect against unauthorized access, use or alteration of Personal Information and Confidential Information and will implement and thereafter maintain safeguards in accordance with agreed upon standard such as (i) the International Organization for Standardization's ISO/IEC 27001:2013 and ISO/IEC 27002:2013 standards or (ii) Health Information Trust Alliance (HITRUST) Certification or (iii) FedRAMP or (iv) DoD Impact Levels, to ensure the security and confidentiality of Personal Information and Confidential Information, protect against any anticipated threats or hazards to the confidentiality, availability or integrity of Personal Information and Confidential Information, and protect against unauthorized access, use, or alteration of Personal Information and Confidential Information. Upon Purchasing Entity's request, Offeror shall promptly and accurately complete a written information security assessment questionnaire provided by Purchasing Entity regarding Offeror's information technology

environment; Offeror will at all times during the Term maintain information security protections no less secure than the practices identified by Offeror in such questionnaire. At a minimum, Offeror shall maintain a comprehensive written information security program managed by one or more designated employees with safeguards that include limiting access to Personal Information and Confidential Information to only employees and authorized Subcontractors who need access to carry out Services under this Agreement, securing business facilities, data centers, paper files, services, back-up systems, computing equipment and mobile devices where Personal Information and Confidential Information is stored, implementing network, device, database and platform security, securing information transmission, storage and disposal, implementing authentication and access controls within media, applications, operating systems and equipment, encrypting sensitive Personal Information (including social security numbers, financial account numbers and health information) during mobile storage and transmission, strictly segregating Personal Information from information of Offeror or its other clients, implementing appropriate personnel security and integrity procedures and practices, providing appropriate privacy and information security training to Offeror's employees and Subcontractors, continually performing self-checks, including, but not limited to scanning for viruses and other contaminants to ensure that such software products have been found to be free of contaminants and viruses identifiable by such scans, and testing against publicized threats, data infiltrations and breaches to ensure the security and confidentiality of Personal Information, and establishing and enforcing written policies regarding the collection, storage, transfer, disclosure, use and disposal of Personal Information and a disciplinary process for employees violating such policies. Offeror shall continually identify and assess reasonably foreseeable internal and external threats and vulnerabilities and, at its sole cost and expense, promptly correct all identified security deficiencies or vulnerabilities that may compromise the security of Personal Information or Confidential Information. Offeror shall also adhere to any of Purchasing Entity's policies, standards, procedures and guidelines provided by Purchasing Entity with respect to the collection, classification and handling of Personal Information and Confidential Information.

d. Data Breaches. Offeror shall immediately notify (within 24 hours) Purchasing Entity if Offeror becomes aware of any accidental or unauthorized disclosure, access or use of any Personal Information or Confidential Information or a violation of applicable privacy or data protection laws (a "Breach") or if Offeror receives an access request, investigative notice, seizure or complaint from a government or data subject related to Purchasing Entity's Confidential Information (unless such notification is prohibited). Offeror shall use its best efforts to immediately remedy any Breach and prevent any further Breach at its sole expense. In the event of any such Breach Offeror shall immediately coordinate with Purchasing Entity regarding the response to, and investigation of, the Breach, and cooperate fully with Purchasing Entity, including facilitating interviews with employees and other parties, making available all relevant records, logs, files, data reporting and other materials, and providing Purchasing Entity with physical access to the facilities affected. In the event of a Breach of Personal Information in Offeror's possession or otherwise caused by or related to Offeror's acts or omissions, and without limiting Purchasing Entity's other rights and remedies, Offeror will pay all reasonable costs and expenses of any disclosures and notification required by applicable law or as otherwise determined as appropriate in Purchasing Entity's reasonable discretion, monitoring and reporting on the impacted individuals' or entities' credit records if determined in Purchasing Entity's reasonable discretion as reasonable to protect such individuals, and all other costs incurred by Purchasing Entity in responding to and mitigating damages caused by such Breach.

e. Cross-Border Transfers. When and as required by Purchasing Entity from time to time, Offeror shall promptly execute and/or shall cause its Affiliate(s) or subcontractor(s) to execute supplemental privacy and security terms, including but not limited to the Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries, dated 5 February 2010 (2010/87/EU), as amended from time to time ("EU Model Contract"), with Offeror or Affiliated companies that provide services under the Agreement as required in Purchasing Entity's sole judgment for the processing and/or transfer of Personal Information in accordance with applicable law. If Offeror will be knowingly transferring Personal Information from, to, or through the European Union, Offeror shall at all relevant times for purposes of this Agreement maintain a current certification status with the US-EU Safe Harbor Privacy Arrangement to protect Personal Information, unless Offeror has notified Purchasing Entity that it does not maintain such a certification and executes an EU Model Contract with Purchasing Entity. Offeror will provide Purchasing Entity with ninety (90) days written notice prior to any date on which Offeror's current Safe Harbor certification status ends.

Audits. Offeror shall comply with all requests from Purchasing Entity to certify Offeror's ongoing compliance with the provisions of this section. Offeror shall provide Purchasing Entity with copies of any applicable Payment Card Industry Data Security Standards (PCI DSS), Statement on Standards for Attestation Engagements No. 16 (SSAE 16), Service Organizations Controls (SOC1, 2 or 3) or Health Insurance Portability and Accountability Act (HIPAA) audits current as of the execution of this Agreement or conducted during the Term. Purchasing Entity reserves the right for it or a third party to conduct a full security audit, assessment or review, including, but not limited to, penetration or vulnerability testing of Offeror's network and systems and physical and technical environment, to identify the strengths and weaknesses of existing security arrangements. Offeror shall fully cooperate with such audit by providing access to knowledgeable personnel, physical premises, documentation and infrastructure unless Offeror security officer reasonably deems such access a threat to Offeror confidentiality and security.

Figure 4 - Armedia Standard Language to Govern Data and Data Breaches

6.3.2 Prohibition of Adware Etc.

8.3.2 Offeror must describe how it will not engage in or permit its agents to push adware, software, or marketing not explicitly authorized by the Participating Entity or the Master Agreement.

ArkCase does not use or permits the use of any adware software as part of the ArkCase SaaS offering.

6.3.3 Testing/Staging Environment

8.3.3 Offeror must describe whether its application-hosting environments support a user test/staging environment that is identical to production.

Armedia uses an on-premise environment for the development and testing of the ArkCase software and has an AWS integration environment where the subsequent product updates and releases are tested. The results of the testing will be made available to the Purchasing Entity with every release of the ArkCase product. Armedia will work with the Purchasing Entity in applying the changes of the subsequent releases to their SaaS offerings.

6.3.4 508 Compliance

8.3.4 Offeror must describe whether or not its computer applications and Web sites are accessible to people with disabilities and must comply with Participating Entity accessibility policies and the Americans with Disability Act, as applicable.

The web interface of ArkCase is compliant with 508 standards making the platform accessible to people with disabilities. Alfresco's 508 compliance is demonstrated in the Voluntary Product Accessibility Template (VPAT). See Appendix A.

6.3.5 Browser Platforms

8.3.5 Offeror must describe whether or not its applications and content delivered through Web browsers are be accessible using current released versions of multiple browser platforms (such as Internet Explorer, Firefox, Chrome, and Safari) at a minimum.

ArkCase ships with an Angular based, responsive web application that can be customized and extended based on the specific requirements of the customer. The web application included with ArkCase works with the latest versions of all known browsers including Internet Explorer, Firefox, Chrome and Safari.

6.3.6 Personal Information

8.3.6 Offeror must describe how it will, prior to the execution of a Service Level Agreement, meet with the Purchasing Entity and cooperate and hold a meeting to determine whether any sensitive or personal information will be stored or used by the Offeror that is subject to any law, rule or regulation providing for specific compliance obligations.

Armedia will facilitate a meeting with Purchasing Entity and cooperate and hold a meeting to determine whether any sensitive or personal information will be stored or used by the Purchasing Entity. In addition, we will document any law, rule or regulation for which we need to comply as well as define information access, retention, and destruction requirements. Figure 4 - Armedia Standard Language to Govern Data and Data Breaches, contains a section that defines PII and will be reviewed and updated pursuant to the meeting with Purchasing Entity.

6.3.7 Project Schedule Plans

8.3.7 Offeror must describe any project schedule plans or work plans that Offerors use in implementing their Solutions with customers. Offerors should include timelines for developing, testing, and implementing Solutions for customers.

ArkCase is offered as SaaS which can be configured by the Purchasing Entities for their customers using the AMI instances provided for ArkCase. Using the setup and installation guide for ArkCase, the Purchasing Entity can provide ArkCase case management platform to its customers with out-of-the-box features shipped in the desired ArkCase model – Basic, Legal or FOIA.

The Purchasing Entity can optionally use Armedia's development and system engineering team's expertise to configure ArkCase for its customers.

Figure 5 - Armedia Development Framework - Framework for extending ArkCase and create specific business extensions as needed

For any custom development of functionalities not included in the ArkCase out-of-the-box offerings, Armedia provides the Armedia Development Framework (ADF - Figure 5) that the Purchasing Entity may use for developing custom business functionality extensions to ArkCase as needed.

Based on our past experiences with our customers like USDA, PAHO etc., Armedia recommends using the proven project development and delivery approached outlined below (Figure 6) when extending ArkCase SaaS and developing custom applications using ArkCase and ADF.

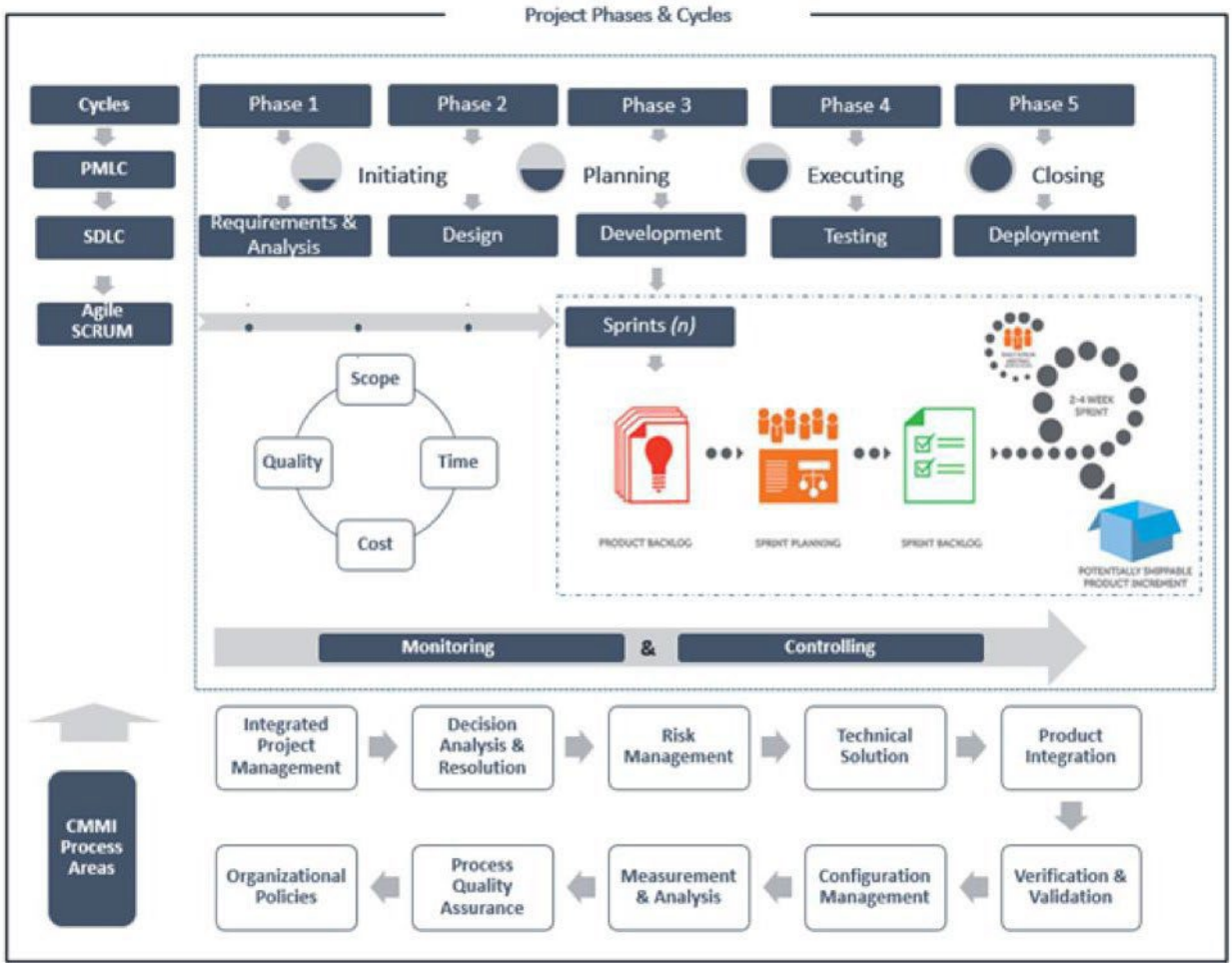


Figure 6 - Armedia's recommended Project Management Plan when developing custom solutions using ADF and ACC

6.3.7.1 Delivery Stages

When Armedia is contracted to develop and deliver custom solutions on behalf of the Purchasing entity, we will fulfill our committed project activities, tasks and deliverables within five **Project Delivery Phases**. The stages and accompanying processes may be *tailored* based on our client's business needs, requirements, operating procedures, or technical environment. A decision whether to adjust Armedia's standard phases and process for any individual client is determined during the Project Kickoff. Following the kickoff, the project moves into the Planning Phase. At that time, the Project Manager creates the defined project processes by tailoring the Armedia standard delivery processes to the client-requested cost, schedule, business, and technical requirements. These tailored processes are documented in the Project Management Plan. The PMP creates a context for the project. It represents agreement with the client on the defined processes.

6.3.7.1.1 Phase 1 – Initiation and Requirements and Analysis

The first delivery Phase consists of the following, initial, high-level project activities.

6.3.7.1.1.1 Project Kickoff

The official start of the project initiates communication and collaboration between the Armedia project team and the system stakeholders. The Project Kickoff meeting solidifies a common understanding of the work, tasks, methodology, and deliverables.

6.3.7.1.1.2 Discovery Workshops

The lead Business Analyst (BA) will schedule workshops (i.e., Joint Application Development – JAD -- sessions) with system stakeholders to review and collect functional and non-functional requirements. The business requirements included in the statement of work will be reviewed, decomposed, and validated with the stakeholders to ensure corporate understanding. In addition, the Armedia team will work closely with the current developers and the stakeholders to ensure a thorough and expedient transition of knowledge occurs.

Following validation of the requirements, the BA will create a Requirements Traceability Matrix (RTM) and (with the project's Technical Lead), perform a gap analysis or reasonability assessment to map the requirements to the system solution. This mapping will identify gaps in the design and/or technology by comparing the known capabilities of the solution and technology with the needs of the stakeholders, as expressed in the requirements. These gaps will then be presented to the stakeholders for further requirements development or mitigation.

6.3.7.1.2 Phase 2 – Planning and Design

The Project Manager plans and schedules the technical activities, producing the Work Breakdown Structure (WBS) and the detailed Project Schedule. The PM creates the defined project processes by tailoring the Armedia standard delivery processes to the system requested cost, schedule, and technical requirements.

6.3.7.1.2.1 Requirements review and preliminary design

The BA and Technical Lead review the RTM. The BA will update any content- or technical-related constraints. When the RTM is agreed to, the Technical Lead creates the conceptual design to include any data and security constraints or concerns, the ITLC security checklist, and the deliverable expectation documentation (DED). The system stakeholders will review and approve the RTM, the conceptual design, and the ITLC checklist, and the DED. Though this is a serial, or waterfall, sequence of events, the entire process may be repeated for each new module or package of system enhancements.

6.3.7.1.2.2 Design

The system requirements are core to the design and engineering of the technical solution. The Technical Lead is responsible for ensuring that the technical solution correctly fits both the system business needs and the operating environment. Team Armedia will update the Design Specification document which may include the system architecture, security, data structures, protocols, components, and interfaces. The system stakeholders will review and approve the Design Specification document before development begins. Though this is a serial, or waterfall, sequence of events, the entire process may be repeated for each new module or package of system enhancements.

6.3.7.1.3 Phase 3 – Development and Execution

The project team will develop, test, and deliver the solution within an Agile sprint-based framework. The Agile approach quickly delivers functionality and actively involves the system stakeholders and users.

6.3.7.1.3.1 Project Management

The PM oversees all project activities, issues, change requests, and risks. The Risk Management Plan is devoted to this critical provision. The PM proactively identifies and mitigates risk from project initiation to closure.

6.3.7.1.3.2 System Engineering

The Armedia System Engineer establishes configuration management processes like source code control, continuous integration, static and dynamic code analysis, automated build and deployments, monitoring, and tuning. Where feasible, these processes will leverage the FDACS Microsoft Team Foundation Server (TFS).

6.3.7.1.3.3 Development

Fully conversant with the system requirements design, the Development Team codes the integrated system components. The team follows the FDACS published Internet web standards for configuration, continuous development, unit testing, and code reviews.

6.3.7.1.3.4 Test

To validate 100 percent requirements coverage, the Testers develop test cases/scripts that map to the system Requirements Traceability Matrix (RTM).

6.3.7.1.4 Phase 4 – Testing

As an overarching *Phase*, monitoring and control is a continuous activity integrated into the entire project life cycle.

6.3.7.1.4.1 Regular Measurement

The Project Manager regularly monitors and takes measurements of the delivery progress. The sooner that the PM can identify variances from the project plan, the less impact they will have. The PM can quickly take corrective action to realign the plan to the project objectives.

6.3.7.1.4.2 Product Control

Testing is our frontline control of product quality. The system solution, as a single functional component, will be tested, verified, and validated against the system requirements. The Test Plan describes the types of tests required (i.e., system integration, performance and user acceptance) and the use of testing tools. Where feasible, all test cases, test data, and test results will be managed in TFS.

6.3.7.1.4.3 Documentation

User documentation will be updated or created to address enhancements to the existing system, and new modules as they are delivered.

6.3.7.1.4.4 User Acceptance Testing

In accordance with the Project Test Plan and the test cases, the Test Team coordinates, supports and executes the System Acceptance and User Acceptance tests. Preparation covers requirements for both internal system testing and external client acceptance testing. The Armedia team follows standard procedure for reporting, correcting, and retesting defects.

6.3.7.1.4.5 Project Financials and Schedule Reporting

Two integrated project plans are appended to the Project Management Plan: Cost Management Plan and Schedule Management Plan. The plans describe the respective monitoring and control guidelines. The Project Manager tracks actual costs and schedule against planned costs and schedule for each Sprint. The PM establishes the metrics and, with the system Project Manager, refines them. Reporting is made monthly.

6.3.7.1.5 Phase 5 – Deployment and Closing

The final Phase formally concludes the system project phase and addresses the activities for turning over the completed solution to the Operations and Maintenance (O&M) team for ongoing support.

6.3.7.1.5.1 System Acceptance

The System Acceptance and Go/No Go criteria is determined during Operations Readiness Review (ORR) meeting with our client's stakeholders, and the Armedia project and Operations and Maintenance (O&M) teams. The purpose of the Operations Readiness Review is to ensure that the project has followed a defined software development process, and that the project team has identified system interdependencies and risks that may have an adverse impact on the organization, and/or the software application/system deployment. The Readiness Review also confirms that appropriate departments have been notified and are fully aware of all pending releases and the potential impact. In this document, risk mitigation strategies and contingency plans are also defined, to help eliminate any adverse impact that may result from the release.

6.3.7.1.5.2 Deployment

In collaboration with the system Project Manager and stakeholders, the Project Manager ensures that 1) system users are properly trained and aware, 2) system technical resources are properly trained and available, and 3) Armedia is fully staffed to provide technical support.

6.3.7.1.5.3 Incident Monitoring

After deploying each component of the system solution, the team will closely monitor incident reports and the Armedia defect tracking database to analyze trends and identify potential enhancements. The PM (or designated team member) will record any resulting enhancements and submit for approval to system, per the established change control process. When approved, these enhancements will be added to the Requirements Traceability Matrix and appropriately scheduled for a release cycle.

6.3.7.1.5.4 Evaluation

In the spirit of project collaboration, Armedia will solicit system user feedback and add it to the solution evaluation report. Our O&M Project Manager and the project team will capture and evaluate lessons learned. Reinforcing our commitment to continuous improvement, we will incorporate into our management processes relevant and constructive findings in the lessons learned and the stakeholder feedback.

6.3.7.1.5.5 Closing

The closing stage of the project includes ensuring all deliverables have been turned over, all contracted obligations have been met, and any lessons learned during the project have been documented for future reference. Knowledge transfer activities should be completed. Any remaining payments or remaining funds should be processed.

6.3.7.2 Delivery Approach

Armedia proposes a hybrid Waterfall-Agile approach, using a Waterfall methodology for the requirements, planning, and high-level design phases, and an Agile methodology for the component design and development phase. We see this approach as beneficial in developing solutions for several reasons. By engaging the stakeholders upfront and early in the process to gather requirements under a Waterfall methodology, Armedia is able to develop a roadmap that

will fully identify and validate the critical business requirements for our client. This will not only produce meaningful milestones but will also set the right expectations.

For development of the custom solutions using ADF and ACC, Armedia proposes an Agile methodology. We will begin with a typical, four-week cycle for each Sprint, but will coordinate with the customer and adjust Sprint durations as necessary to meet the demands of the project. Each Sprint will provide business owners and users with a one-week validation of the functionality of the Sprint. This method will benefit our client by providing continuous feedback and allow the Armedia development team to promptly address feedback.

6.3.8 Service Updates

8.3.8 The State of Utah expects Offeror to update the services periodically as technology changes. Offer must describe:

- *How Offeror's services during Service Line Additions and Updates pursuant to section 2.12 will continue to meet the requirements outlined therein.*

Armedia is committed to providing great service to its customers through continuous improvements and innovations on ArkCase. Armedia development teams work directly with customers to ensure that innovation on the ArkCase platform is driven by customer demand, and we continuously evolve and improve our existing services and frequently add new services. Armedia's typical release cycle is 3-6 months for minor releases and 18-24 months for major releases. Patch releases to address an immediate concern are also scheduled. To attract and retain Purchasing Entities, Armedia understands that Purchasing Entities have options and we must provide compelling offerings that are secure, intuitive, modern and flexible to support a fluid environment.

While Armedia continues development of ArkCase software, the Purchasing Entities will have access to the ArkCase release plans as well as release notes.

Self-Managed ArkCase SaaS	Fully-Managed ArkCase SaaS
Armedia will provide the Purchasing Entity with the ArkCase release plans. The Purchasing Entity will be responsible for upgrading the SaaS for their customers based on their contract agreements.	Armedia will communicate with the Purchasing Entity and its customers of the ArkCase release cycles as well as provide security and patch updates. Armedia recommends forming a Change Control Board comprising of the Purchasing Entity its customers and having periodic scheduled meetings to communicate all software and patch releases with the CCB before it is applied.

- *How Offeror will maintain discounts at the levels set forth in the contract.*

As with Armedia's GSA Schedules that Armedia has maintained for over ten years, Armedia will maintain discounts as the levels set forth in the contract.

- *How Offeror will report to the Purchasing Entities, as needed, regarding changes in technology and make recommendations for service updates.*

Armedia provides periodic updates to ArkCase. These updates along with the release notes will be made available to the Purchasing Entities and their customers. The Purchasing Entity will be responsible of applying these updates to their applications developed using ADF for their customers at their discretion.

- *How Offeror will provide transition support to any Purchasing Entity whose operations may be negatively impacted by the service change.*

Any updates made to ArkCase – that includes applying security patch releases to the ArkCase components that may impact the Purchasing Entity – will be communicated with the Purchasing Entity along with the expected service outage time if any.

6.4 Customer Service

ENSURING EXCELLENT CUSTOMER SERVICE

8.4.1 Offeror must describe how it will ensure excellent customer service is provided to Purchasing Entities. Include:

- *Quality assurance measures;*
- *Escalation plan for addressing problems and/or complaints; and*
- *Service Level Agreement (SLA).*

8.4.2 Offeror must describe its ability to comply with the following customer service requirements:

- *You must have one lead representative for each entity that executes a Participating Addendum. Contact information shall be kept current.*
- *Customer Service Representative(s) must be available by phone or email at a minimum, from 7AM to 6PM on Monday through Sunday for the applicable time zones.*
- *Customer Service Representative will respond to inquiries within one business day.*
- *You must provide design services for the applicable categories.*
- *You must provide Installation Services for the applicable categories.*

Armedia's technical support for ArkCase SaaS is a one-on-one, fast-response support channel that is staffed 24x7x365 with AWS certified and experienced technical support engineers. The service helps customers of all sizes and technical abilities to successfully use ArkCase for basic, legal and FOIA implementations.

Armedia also provides training modules and instruction vidoes for ArkCase to its customers that help them get familiar with the workings of the product. Additionally, ArkCase setup, installation and administrator guides are provided to the Purchasing Entities to help setup and manage ArkCase SaaS for their customers.

Armedia also provides detailed release notes with every release of the ArkCase SaaS platform along with the code quality coverage reports and test results as part of Armedia Qaulity Assurance for the ArkCase SaaS offering.

Armedia Support Features for ArkCase SaaS

Armeida Support provides a highly personalized level of service for customers seeking technical help. Customers who do not choose Armedia Support will continue to have access to Basic Support offered at no additional charge. Besides the Basic Support – included with the ArkCase SaaS offering – Armedia offers a flat rate support plan (Enterprise Support) for ArkCase that is available to the Purchasing Entities on a monthly subscription basis. All plans, including Basic Support, provide 24x7 access to customer service, ArkCase Documentation, Resource Center, Product Wiki and FAQs, Discussion Forums, and support for Health Checks.

Contacting Armedia Support

Customers can contact Armedia Support via the Support Center. All Developer-level support customers can open a case online using a web browser. Customers with a paid enterprise support subscription will be able to call Armedia Support or strike up a conversation with an engineer via Chat.

Chat is another way to contact Armedia Support. By clicking on the chat support icon in the Support Center, a chat session will be initiated through the browser. This provides a real-time, one-on-one interaction with our support engineers and allows additional information and links to be shared for faster issue resolution.

	Basic	Enterprise
Customer Service – 24x7x365	✓	✓
Support Forums	✓	✓
Documentation, Whitepapers, Best Practice Guides	✓	✓
Access to Technical Support	Support for Health Checks	Phone, Chat, Email, Technical Account Manager (TAM) (24/7)
Primary Case Handling	Technical Customer Service Associate	ArkCase SaaS support engineer
Users Who Can Create Technical Support Cases		5
Response Time		General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour Business-critical system down: < 15 minutes
Architecture Support		Contextual Application Architecture Guidance
Access to Support API		✓
Third-Party Software Support		✓
Infrastructure Event Management		Contact us for pricing
Architectural Review		✓

	Basic	Enterprise
Support Concierge		✓
Training	Online training videos	Online training videos
Operations Support		Operational reviews, recommendations, and reporting

6.5 Security of Information

6.5.1 Protection of Data

8.5.1 Offeror must describe the measures it takes to protect data. Include a description of the method by which you will hold, protect, and dispose of data following completion of any contract services.

Data in Armedia's PaaS and SaaS offerings is protected through a number of means including, but not limited to data encryption (including encryption of data both in transit and at rest), access control, system integrity protection (to protect against and protect from threats such as malware), and network-level defenses (to protect against and protect from network-based attacks). Following the completion of any contract services, Armedia will hold, protect, transfer or dispose of applicable customer data as appropriate. This will be achieved through the following process:

- Identification of customer data requirements beyond those already identified
- Archiving of any data required by the customer for duration specified by the Purchasing Entity and their customers using Amazon Glacier
- Secure transfer of archived data to the customer as required using Amazon's bulk data transfer tool – AWS Import/Export Disk and AWS Snowball Edge – a data transport solution that uses devices designed to be secure to transfer large amounts of data into and out of the AWS Cloud.
- Deletion of customer data from Armedia PaaS and/or SaaS systems using the AWS techniques compliant with the process detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.
- Deletion of customer data from Armedia-controlled backup that is built on AWS Glacier and DR systems when the Purchasing Entity uses a DR setup for the ADF based custom applications.

6.5.2 Compliance with Data Privacy/Security Regulations

8.5.2 Offeror must describe how it intends to comply with all applicable laws and related to data privacy and security.

Armedia uses FedRAMP security controls as the baseline for its security testing for ArkCase. The Purchasing Entities are open to design additional security controls that comply with all applicable laws and regulations related to data privacy and security for its customers as needed. In the event of Armedia being contracted to develop custom solutions for the Purchasing Entity that extends ArkCase using ADF, Armedia will work with the Purchasing Entity to comply with any additional security controls not already covered by the FedRAMP controls. The process utilized for this consists of the following:

- Identification of applicable laws and regulations with customers during project specification
- Identification of any gaps in PaaS and/or SaaS processes due to laws and regulations identified in the previous step
- Modification of processes as required in order to achieve full compliance with applicable laws and regulations related to data privacy and security

6.5.3 Purchasing Entity's User Accounts

8.5.3 Offeror must describe how it will not access a Purchasing Entity's user accounts or data, except in the course of data center operations, response to service or technical issues, as required by the express terms of the Master Agreement, the applicable Participating Addendum, and/or the applicable Service Level Agreement.

Armedia personnel will not access any Purchasing Entity's user accounts or data, except in the course of data center operations, response to service or technical issues, as required by the express terms of the Master Agreement, the applicable Participating Addendum, and/or the applicable Service Level Agreement. Armedia systems are designed with a *least privilege* philosophy, which limits Armedia personnel access to customer data through technical control methods such as access control. Additionally, Armedia personnel are barred by Armedia policy from accessing customer data for any unauthorized purposes. Also, all customer data on ACC is stored on encrypted storage devices providing additional data security at rest.

6.6 Privacy and Security

6.6.1 NIST Compliance

*8.6.1 Offeror must describe its commitment for its Solutions to comply with NIST, as defined in NIST Special Publication 800-145, and any other relevant industry standards, as it relates to the Scope of Services described in **Attachment D**, including supporting the different types of data that you may receive.*

Armedia's PaaS and SaaS offerings are designed and operated as cloud-based services, as defined in NIST Special Publication 800-145. In addition, Armedia follows applicable information security controls for a Moderate impact system from NIST Special Publication 800-53 as a configuration, architectural, and operational baseline.

6.6.2 Security Certifications

8.6.2 Offeror must list all government or standards organization security certifications it currently holds that apply specifically to the Offeror's proposal, as well as those in process at time of response.
Specifically include HIPAA, FERPA, CJIS Security Policy, PCI Data Security Standards (DSS), IRS Publication 1075, FISMA, NIST 800-53, NIST SP 800-171, and FIPS 200 if they apply.

A CSA STAR self-assessment has been completed for Armedia's PaaS and SaaS offerings, and the results of that self-assessment are attached to this response.

A third-party assessment organization has completed assessment of Armedia's FedRAMP offering, and Armedia anticipates a full FedRAMP authorization for said offering by September 2018. https://marketplace.fedramp.gov/#/product/armedia-content-cloud?sort=productName.

ArkCase SaaS is built and deployed using NIST 800-53 compliant AWS resources and infrastructure that has been designed and is managed in alignment with regulations, standards, and best practices, including:

- Federal Risk and Authorization Management Program (FedRAMP)
- National Institute of Standards and Technology (NIST) 800-171
- Federal Information Security Management Act (FISMA)
- Federal Information Processing Standard (FIPS) 140-2
- Department of Defense (DoD) Security Requirements Guide (SRG) Impact Levels 2, 4, 5, and 6
- FBI Criminal Justice Information Services (CJIS)
- US Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)
- International Organization for Standardization (ISO) 27001, 27017, 27018, and 9001
- International Traffic in Arms Regulations (ITAR)
- Family Educational Rights and Privacy Act (FERPA)
- System and Organization Controls (SOC) 1, SOC 2, and SOC 3

6.6.3 Security Practices

8.6.3 Offeror must describe its security practices in place to secure data and applications, including threats from outside the service center as well as other customers co-located within the same service center.

Armedia follows industry standard best practices in the area of information security, and manages environments with a range of specific security requirements including compliance with:

- FedRAMP Moderate
- HITRUST
- HIPAA
- CJIS

Physical security for Armedia's PaaS and SaaS offerings is managed by Amazon, as all environments are hosted within AWS.

Protection of data from other ArkCase customers is accomplished through the use of AWS VPCs and AWS security groups. AWS security monitoring tools help identify several types of denial of service (DoS) attacks, including distributed, flooding, and software/logic attacks. When DoS attacks are identified, the AWS incident response process is initiated. In addition to the DoS prevention tools, redundant telecommunication providers at each region as well as additional capacity protect against the possibility of DoS attacks.

ArkCase SaaS's use of AWS network provides significant protection against traditional network security issues, and you can implement further protection. The following are a few examples:

- **Distributed Denial of Service (DDoS) Attacks.** AWS API endpoints are hosted on large, Internet-scale, world-class infrastructure that benefits from the same engineering expertise that has built Amazon into the world's largest online retailer. Proprietary DDoS mitigation techniques are used. Additionally, AWS's networks are multi-homed across a number of providers to achieve Internet access diversity.
- **Man in the Middle (MITM) Attacks.** All of the AWS APIs are available via SSL-protected endpoints which provide server authentication. Amazon EC2 AMIs

automatically generate new SSH host certificates on first boot and log them to the instance's console. You can then use the secure APIs to call the console and access the host certificates before logging into the instance for the first time. We encourage you to use SSL for all of your interactions with AWS.

- **IP Spoofing.** Amazon EC2 instances cannot send spoofed network traffic. The AWS-controlled, host-based firewall infrastructure will not permit an instance to send traffic with a source IP or MAC address other than its own.
- **Port Scanning**. Unauthorized port scans by Amazon EC2 customers are a violation of the AWS Acceptable Use Policy. Violations of the AWS Acceptable Use Policy are taken seriously, and every reported violation is investigated. Customers can report suspected abuse via the contacts available on our website at: http://aws.amazon.com/contact-us/report-abuse/. When unauthorized port scanning is detected by AWS, it is stopped and blocked. Port scans of Amazon EC2 instances are generally ineffective because, by default, all inbound ports on Amazon EC2 instances are closed and are only opened by you. Your strict management of security groups can further mitigate the threat of port scans. If you configure the security group to allow traffic from any source to a specific port, then that specific port will be vulnerable to a port scan. In these cases, you must use appropriate security measures to protect listening services that may be essential to their application from being discovered by an unauthorized port scan. For example, a web server must clearly have port 80 (HTTP) open to the world, and the administrator of this server is responsible for the security of the HTTP server software, such as Apache. You may request permission to conduct vulnerability scans as required to meet your specific compliance requirements. These scans must be limited to your own instances and must not violate the AWS Acceptable Use Policy. Advanced approval for these types of scans can be initiated by submitting a request via the website at: https://aws-portal.amazon.com/gp/aws/html-forms-controller/contactus/AWSSecurityPenTestRequest
- **Packet sniffing by other tenants.** It is not possible for a virtual instance running in promiscuous mode to receive or "sniff" traffic that is intended for a different virtual instance. While you can place your interfaces into promiscuous mode, the hypervisor will not deliver any traffic to them that is not addressed to them. Even two virtual instances that are owned by the same customer located on the same physical host cannot listen to each other's traffic. Attacks such as ARP cache poisoning do not work within Amazon EC2 and Amazon VPC. While Amazon EC2 does provide ample protection against one customer inadvertently or maliciously attempting to view another's data, as a standard practice you should encrypt sensitive traffic.

6.6.4 Data Confidentiality

8.6.4 Offeror must describe its data confidentiality standards and practices that are in place to ensure data confidentiality. This must include not only prevention of exposure to unauthorized personnel, but also managing and reviewing access that administrators have to stored data. Include information on your hardware policies (laptops, mobile etc).

Armedia does not access the Purchasing Entity or their customer's data, and the Purchasing Entity is given the choice as to how they store, manage and protect their data.

Armedia ensures data confidentiality in its PaaS and SaaS offerings through means including the use of technical and policy access control measures. Armedia systems are architected using a *least privilege* philosophy. Access privileges granted to Armedia administrators are reviewed on at least an annual basis. Data in Armedia environments is securely encrypted, both in transit and at rest.

Armedia issues laptops to its employees and said laptops are used for tasks such as management of Armedia environments. Armedia environments are not managed through the use of personally owned mobile devices.

6.6.5 Third Party Security Credentials

8.6.5 Offeror must provide a detailed list of the third-party attestations, reports, security credentials (e.g., FedRAMP High, FedRAMP Moderate, etc.), and certifications relating to data security, integrity, and other controls.

Armedia currently has In Process designation from the FedRAMP PMO for a FedRAMP Moderate Impact offering.

A third-party assessment organization has completed assessment of Armedia's FedRAMP offering, and Armedia anticipates a full FedRAMP authorization for said offering by September 2018. https://marketplace.fedramp.gov/#/product/armedia-content-cloud?sort=productName.

6.6.6 Logging Process

8.6.6 Offeror must describe its logging process including the types of services and devices logged; the event types logged; and the information fields. You should include detailed response on how you plan to maintain security certifications.

ArkCase utilizes ELK (Elasticsearch/Logstash/Kibana) for log archiving, analysis, and correlation. Armedia's implementation of ELK ingests log information from applications, network devices, databases, and operating systems in all systems in Armedia's offerings. Specific log information collected within ELK includes, but is not limited to the following:

- Successful and unsuccessful account logon events
- Account management events
- Object access
- Policy change
- System events
- Administrator activity
- Authentication checks
- Authorization checks
- Data deletions
- Data access
- Data changes
- Permission changes

Information stored in ELK for Armedia's offerings is stored in a read-only format, and access is limited to authorized personnel only. These protections help to ensure that log data cannot be modified in order to certify the accuracy and integrity of the log data stored within ELK.

ArkCase logging can be configured using a logging configuration dashboard accessible only to authorized personnel through role-based access controls (Figure 7).

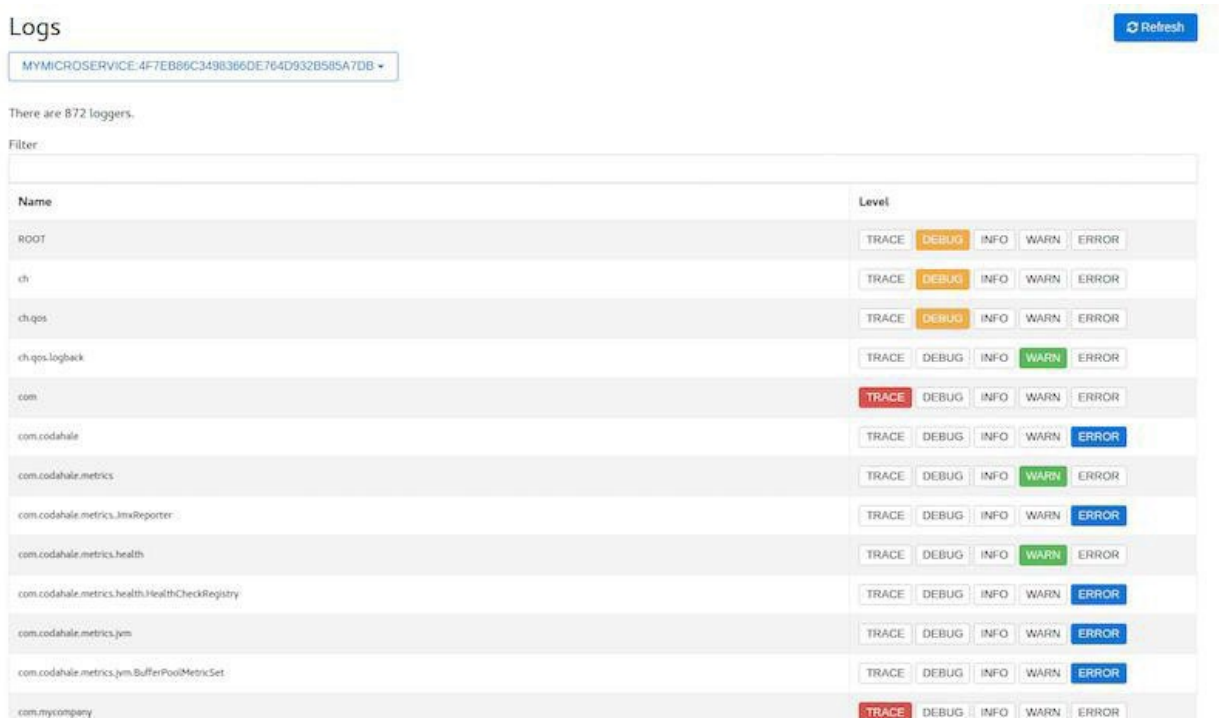


Figure 7 - Configuring logging for ArkCase

6.6.7 Visibility of Data

8.6.7 Offeror must describe whether it can restrict visibility of cloud hosted data and documents to specific users or groups.

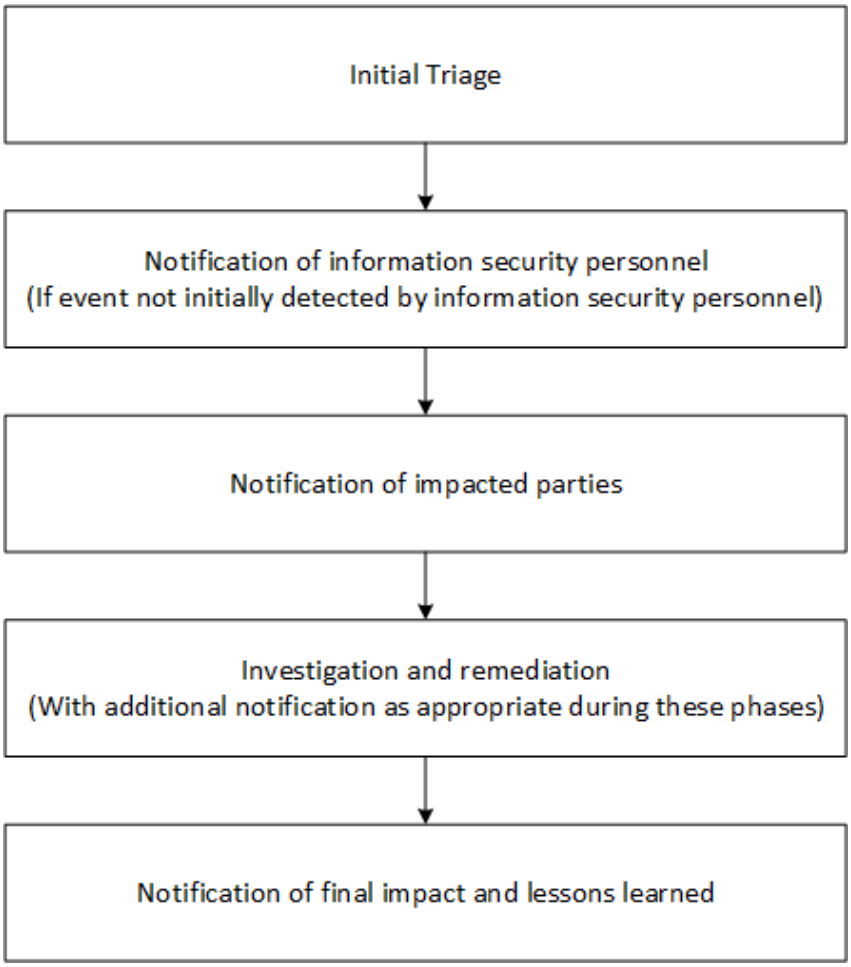
Armedia's PaaS and SaaS offerings provide the ability to restrict visibility of data and documents to specific users and groups. This is achieved through the use of role-based access control in said offerings. Customer environments are segregated from one another utilizing dedicated customer VPCs and AWS Security Groups. Additionally, multifactor authentication can be provided for customer environments in order to provide an additional level of data protection.

6.6.8 Notification Process

8.6.8 Offeror must describe its notification process in the event of a security incident, including relating to timing, incident levels. Offeror should take into consideration that Purchasing Entities may have different notification requirements based on applicable laws and the categorization type of the data being processed or stored.

The customer notification process utilized by Armedia for its PaaS and SaaS offerings in the event of a security incident are as follows:

- Initial triage of the event
- Notification of information security personnel if event not initially detected by information security personnel
- Notification of impacted parties (by email and/or phone depending upon specific requirements)
- Investigation and remediation (with additional notification as appropriate during these phases)
- Notification of final impact and lessons learned.



Specific timelines for each of these steps are dependent upon individual customer requirements and Service Level Agreements.

Additionally, ACC uses AWS notification mechanisms (AWS SNS and email) that are in place to allow the customer support team to be notified of operational issues that impact the customer experience. A "Service Health Dashboard" is available and maintained by the customer support team to alert customers to any issues that may be of broad impact.

6.6.9 Security on Hosted Servers

8.6.9 Offeror must describe and identify whether or not it has any security controls, both physical and virtual Zones of Control Architectures (ZOCA), used to isolate hosted servers.

ArkCase SaaS uses the AWS environment which is a virtualized, multi-tenant environment. ArkCase SaaS relies on AWS implemented security management processes, PCI controls, and other security controls designed to isolate each customer from other customers. ArkCase SaaS's use of AWS systems is designed to prevent customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software. This architecture has been validated by an independent PCI Qualified Security Assessor (QSA) and was found to be in compliance with all requirements of PCI DSS version 3.2 published in April 2016.

ArkCase SaaS also supports AWS single-tenancy options. Dedicated Instances are Amazon EC2 instances launched within your Amazon Virtual Private Cloud (Amazon VPC) that run hardware

dedicated to a single customer. Dedicated Instances let you take full advantage of the benefits of Amazon VPC and the AWS Cloud while isolating your Amazon EC2 compute instances at the hardware level.

Servers utilized for ArkCase platform are deployed on a customer-by-customer basis, with each customer environment being deployed in separate VPCs (Virtual Private Clouds) within AWS. These VPCs are protected through use of AWS Security Groups, which provide firewall-like functionality. Security Groups for VPCs in Armedia's offerings are deployed using a deny-all philosophy, in which network access to systems and groups of systems is denied by default, and network access to systems and services must be explicitly authorized.

6.6.10 Security Technical Reference Architectures

8.6.10 Provide Security Technical Reference Architectures that support Infrastructure as a Service (IaaS), Software as a Service (SaaS) & Platform as a Service (PaaS).

The ArkCase SaaS platform is designed to be deployed in a multi-zonal ACC environment that places high value on data security (Figure 8). It uses AWS encrypted data stores providing data security at rest and uses TLS 1.2 and SSH configured using strong cipher suites for protecting the data in transit.

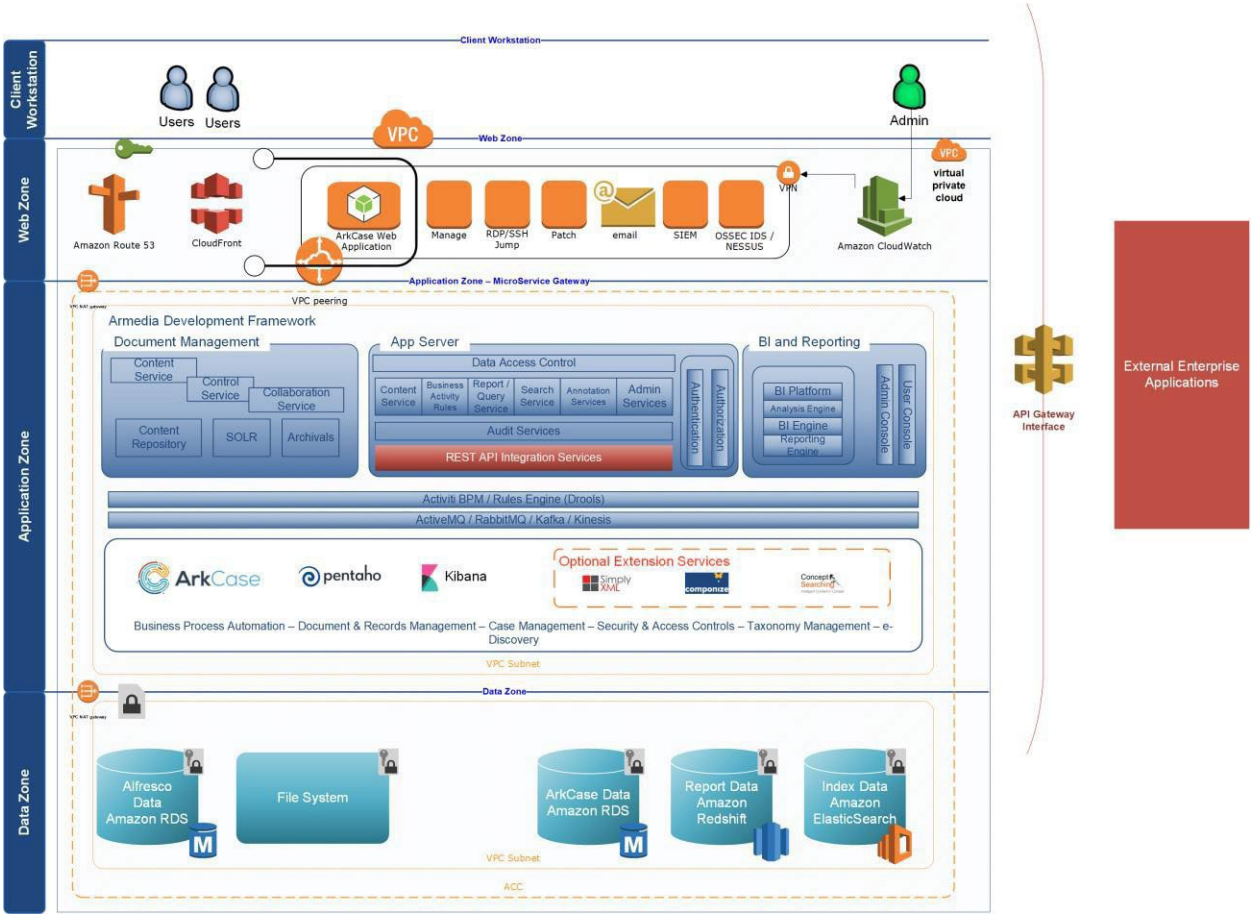


Figure 8 - Multi-zonal ADF architecture with distinct VPC subnets for data security

The architecture is comprised of a web zone, application zone, and data zone where each is separated and protected by firewalls and access policies.

- Web-zone – Hosts the web application built on Angular that facilitates user interactions with the ArkCase SaaS platform. This interface uses secure transport layer (HTTPS) protocols to securely transmit data between the end users and the ArkCase SaaS platform. The HTTPS transport layer uses trusted PKI certificates to encrypt and secure any data transmitted from the browsers to the ArkCase SaaS platform. The web application interface also employs a responsive design making the interface workable on desktop as well as mobile devices.
- Application Zone – Hosts multiple components of the business application based on ADF – the main ArkCase application server (a Java-Spring framework based middleware application with Spring Security and Java cryptographic libraries), Alfresco Content Services, Alfresco Activiti business process management (BPM) components. ArkCase application provides services that includes, but are not limited to
    - Incident management module
    - Case management module
    - Document and Records management module
    - Reporting module
    - Security and role-based access controls
    - Forms module
    - Annotation and redaction module
    - Communications module
    - Business rules module
    - Full text-search module
    - Auditing module
    - Analytics and BI dashboard module
    - An enterprise service bus (ESB) module
- Data Zone – Hosts the application database utilizing encrypted data stores for sensitive information, Alfresco content store (also encrypted) for storing various documents and records as it relates to the ArkCase SaaS application, file server for facilitating uploads of documents and virus scanning before it gets stored in the Alfresco ECM.
- External Interfaces – These are the external applications that the ArkCase SaaS platform will integrate with through its representational state transfer (REST) / service-oriented architecture (SOA) application programming interfaces (APIs). The known applications include FMS, NTI, SMART, HR etc. ArkCase uses ActiveMQ - the leading open source integration platform as the orchestration engine for external interfaces.

ArkCase SaaS's multi-zonal architecture provides independent scalability at each zone of the SaaS platform. This approach provides granular control and configuration options on how the platform can meet growth demands.

Figure 9 depicts a sample ACC setup for ArkCase based application developed and maintained by Armedia for Pan-America Health Organization.

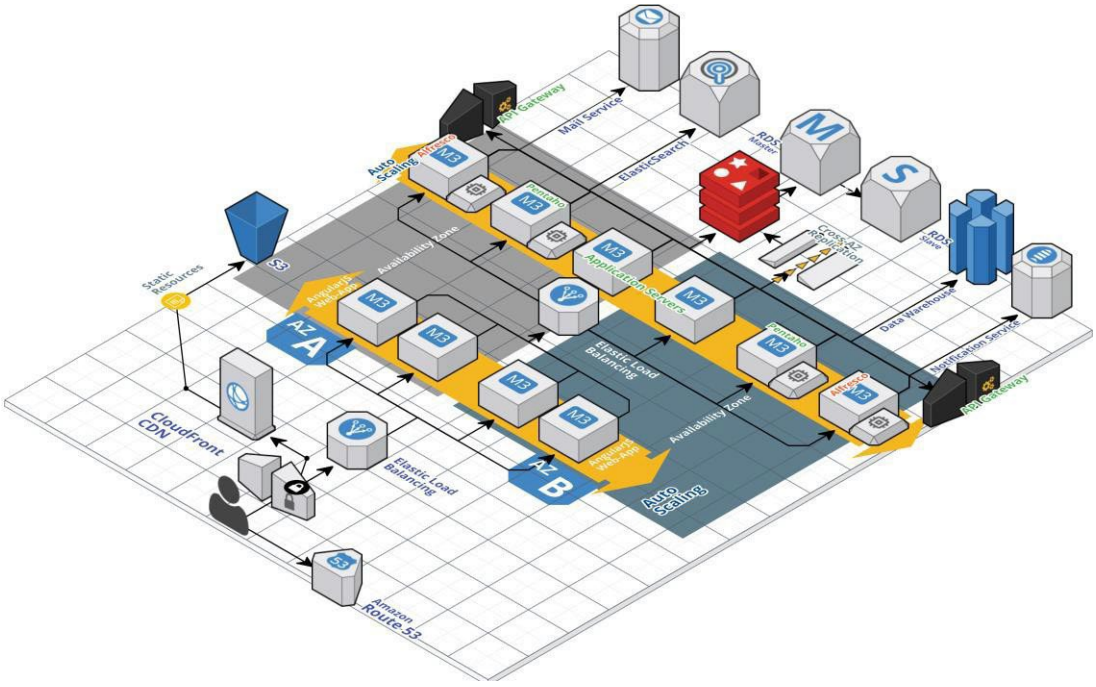


Figure 9 - ACC architecture for ArkCase based applications using a High-Availability, High-Scalability configuration

The Purchasing Entities retain the responsibility to create, setup and monitor their own environments that they manage for their customers. Armedia offers sample architecture recommendations for ArkCase deployed on ACC (Figure 9).

Armedia's security implementation utilizes a standardized reference architecture, in which the following functionality is deployed in all Armedia PaaS and SaaS offerings:

- Authentication and Authorization (Currently utilizing Active Directory for authentication/authorization)
- Network Protection (Currently utilizing AWS Security Groups and AWS DoS protection for network protection)
- System and Service Hardening (Currently using CIS Benchmarks and DISA STIGs as configuration baselines)
- File Integrity Monitoring (Currently utilizing OSSEC for file integrity monitoring)
- Host-based Intrusion Detection (Currently utilizing OSSEC for file integrity monitoring)
- Malware Detection/Protection (Currently utilizing Trend Micro and ClamAV for malware detection and protection)
- Log Analysis and Correlation (Currently utilizing ELK for log archiving, analysis, and correlation)
- Vulnerability Management (Currently utilizing Tenable Nessus for vulnerability detection)

6.6.11 Security Procedures for Employees

8.6.11 Describe security procedures (background checks, foot printing logging, etc.) which are in place regarding Offeror's employees who have access to sensitive data.

Armedia employees undergo successful background and drug checks prior to employment. Armedia employees do not have physical access to any of the systems, as Armedia's PaaS and SaaS offerings are entirely hosted on Amazon Web Services. Once employed, Armedia facilities are controlled by a badging system so public users cannot enter our work space. In addition,

employees must authenticate to gain access to systems within the domain and once authenticated, user actions are logged for auditing.

Armedia will meet with Purchasing Entity to review our Security Procedures and if additional measures are necessary, we will implement them for employees accessing the Purchasing Entities systems and data. Armedia is accustomed to operating in this manner for our commercial and government clients with specific requirements (i.e. Top-Secret, CJIS, etc.)

6.6.12 Confidentiality of Data

8.6.12 Describe the security measures and standards (i.e. NIST) which the Offeror has in place to secure the confidentiality of data at rest and in transit.

Armedia utilizes encryption methods compliant with the requirements of NIST Special Publication 800-53 Rev4 and industry best practices in order to protect the confidentiality of customer information at rest and in transit. Specifically, data in transit for Armedia's PaaS and Sass offerings is protected using encryption technologies including:

- TLS (utilizing only TLS versions 1.1 and 1.2)
- SSH

Additionally, TLS and SSH are configured to only utilize strong cipher suites for the protection of information in transit.

File-level data at rest is stored on encrypted AWS EBS volumes. Database information at rest is stored in AWS RDS encrypted databases. Archived data is stored in encrypted AWS S3 buckets and AWS Glacier. All data at rest is encrypted using AWS-provided encryption methods, which utilize AES-256 encryption.

6.6.13 Notification in the Event of a Data Breach

8.6.13 Describe policies and procedures regarding notification to both the State and the Cardholders of a data breach, as defined in this RFP, and the mitigation of such a breach.

In the event of a data breach, Armedia would notify customers impacted by said breach using the following process:

- Initial triage of the event
- Notification of information security personnel if event not initially detected by information security personnel
- Notification of impacted parties (by email and/or phone depending upon specific requirements)
- Investigation and remediation (with additional notification as appropriate during these phases)
- Notification of final impact and lessons learned.

Customer notification timelines would be dependent upon specific customer requirements and would be established with each customer prior to customer systems being placed in production. Armedia does not normally access individual customer information, so it would not have access to individual Cardholder information. As a result, Cardholder notification would be considered a customer responsibility, although Armedia will provide assistance to Customers during the notification process.

6.7 Migration and Redeployment Plan

6.7.1 Closing Down a Service

8.7.1 Offeror must describe how it manages the end of life activities of closing down a service to a Purchasing Entity and safely deprovisioning it before the Offeror is no longer contractually obligated to maintain the service, include planned and unplanned activities. An Offeror's response should include detail on how an Offeror maintains security of the data during this phase of an SLA, if the Offeror provides for redundancy during migration, and how portable the data is during migration.

Armedia is committed to working with the Purchasing Entity on closing down of ArkCase SaaS offering as per the agreement with the Purchasing Entity. When Armedia is contracted to manage ArkCase SaaS on behalf of the Purchasing Entity, Armedia will provide and update the Purchasing Entity with the service closing process documentation and will transfer all the data to the Purchasing Entity and its customer as agreed in the contract. Armedia ensures total shutdown and termination of services including deleting all associated data on ArkCase SaaS once the data transfer is completed after service closure.

In all other cases, the Purchasing Entities manage the creation and deletion of their data on ArkCase SaaS, as well as maintain control of access permissions. The Purchasing Entities are responsible for maintaining appropriate data retention policies and procedures. The Purchasing Entities in place limit access to systems and data and provide that access to systems or data is restricted and monitored. In addition, customer data and server instances are logically isolated from other customers by default. Privileged user access control is reviewed by an independent auditor during the AWS SOC 1, ISO 27001, PCI, and FedRAMP audits.

The closing down of the service and its activities will depend on the SaaS model chosen – self-managed or fully-managed. Since ArkCase SaaS is setup using independent AMI instances for each customer, the closing down the service entails terminating the AMI instance and relinquishing all the AWS resources including disks, block storage volumes, EC2 instances etc. along with terminating the underlying services like the AWS RDS and AWS ElasticSearch.

Self-Managed ArkCase SaaS	Fully-Managed ArkCase SaaS
The Purchasing Entity will define the closing down process with its customers and be responsible for all the closing down activities.	Armedia will terminate the AWS ArkCase instances and transfer the data to the Purchasing Entity and/or its customers before destroying the data as per agreed contract.
The Purchasing Entity will be responsible for any data transfer and data purging at the closing of the service.	Armedia will use AWS Snowball data transfer service to transfer customer data securely to the customer as required.

6.7.2 The Return of Data

8.7.2 Offeror must describe how it intends to provide an orderly return of data back to the Purchasing Entity, include any description in your SLA that describes the return of data to a customer.

In the case where Armedia is contracted to setup and manage ArkCase SaaS on behalf of the Purchasing Entity, Armedia agrees to return all data back to the Purchasing Entity using AWS Import/Export Disk and AWS Snowball Edge service to ensure secure data transfer. Transferring data with AWS Import/Export Disk and AWS Snowball Edge is simple, fast, more secure, and can be as little as one-fifth the cost of transferring data with a high-speed Internet.

In all other cases, the Purchasing Entities are responsible for managing their data.

Self-Managed ArkCase SaaS	Fully-Managed ArkCase SaaS
The Purchasing Entity owns the access to the data.	Armedia will use AWS Import/Export Disk and AWS Snowball Edge data transfer service to transfer customer data securely to the customer as agreed in the SLA.

6.8 Service or Data Recovery

6.8.1 Responses

8.8.1 Describe how you would respond to the following situations; include any contingency plan or policy.
a. Extended downtime.
b. Suffers an unrecoverable loss of data.
c. Offeror experiences a system failure.
d. Ability to recover and restore data within 4 business hours in the event of a severe system outage.
e. Describe your Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

ArkCase SaaS uses ACC that is based on Amazon's infrastructure which has a high level of availability and provides customers the features to deploy a resilient IT architecture. Armedia has designed its ArkCase SaaS platform on ACC to tolerate system or hardware failures with minimal customer impact.

a. ***Extended Downtime***

ArkCase SaaS deployed on ACC is architected and designed to take advantage of multiple AWS regions and AWS availability zones (Figure 2). Distributing applications across multiple availability zones provides the ability to remain resilient in the face of most failure modes, including natural disasters or system failures.

b. Loss of Data

ArkCase SaaS deployment on ACC using AWS infrastructure that takes advantage of multiple AWS regions and availability zones provides resilience to loss of data due to system failure through having copies of data across regions and availability zones. ACC also creates periodic backup snapshots of the system that can be used for recovery of data.

Additionally, when contracted to setup and manage ArkCase SaaS on behalf of the Purchasing Entity, Armedia provides the option of using a disaster recovery (DR) setup along with the high-availability, high-resilient setup for its solutions at an additional service cost to the Purchasing Entity. Armedia takes full responsibility of maintaining the data copies at the DR with snapshots of data and the applications taken at regular intervals in a manner that would minimize unrecoverable loss of data.

In all other cases, the Purchasing Entities are responsible for protecting against unrecoverable loss of data through their own DR and data recovery mechanisms.

c. System Failures

ArkCase SaaS infrastructure is guaranteed by the AWS SLAs that account for any system failures.

d. Data Recovery

The time of data recovery varies and is dependent on the total volume of data being recovered as well as the method of data recovery – recovery from a passive DR instance (shorter recovery time) vs recovery from cold backups (longer recovery time).

6.8.2 Backup and Restore Services

8.8.2 Describe your methodologies for the following backup and restore services:
a. Method of data backups
b. Method of server image backups
c. Digital location of backup storage (secondary storage, tape, etc.)
d. Alternate data center strategies for primary data centers within the continental United States

When contracted to setup and manage ArkCase SaaS on behalf of the Purchasing Entity, Armedia provides the option of using a disaster recovery (DR) setup along with the high-availability, high-resilient setup for its solutions at an additional service cost to the Purchasing Entity. Armedia takes full responsibility of maintaining the data copies at the DR with syncing of data and the applications at regular intervals in a manner that would minimize unrecoverable loss of data.

Armedia also creates backup of data stored on AWS EBS by taking point-in-time snapshots that can be used to restore data in case of a disk volume failure.

Purchasing entities have options to create DR sites using different AWS regions – geographically separated across the globe based on the data retention and management policies. AWS currently has 18 regions, 54 Availability Zones, and 1 Local Region throughout the world: US East (Northern Virginia), US East (Ohio), US West (Oregon), US West (Northern California), AWS GovCloud (US-West), Canada (Central), EU (Ireland), EU (Frankfurt), EU (London), EU (Paris), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), Asia Pacific (Seoul), Asia Pacific (Mumbai), Asia Pacific (Osaka-Local), South America (Sao Paulo), China (Beijing), and China (Ningxia). Information on each region can be found at the AWS Global Infrastructure webpage.

6.9 Data Protection

6.9.1 Methodology

8.9.1 Specify standard encryption technologies and options to protect sensitive data, depending on the particular service model that you intend to provide under this Master Agreement, while in transit or at rest.

Securing Data at Rest

ArkCase SaaS supports multiple options for encrypting data at rest, ranging from completely automated encryption solutions (using AWS Key Management Service [KMS]) to manual, client-side options (using AWS CloudHSM). The Purchasing Entity can choose the option based on the customer requirements for key management.

Securing Data in Transit

Protecting data in transit when running applications in the cloud involves protecting network traffic between clients and servers and network traffic between servers.

ArkCase SaaS provides support for both Internet Protocol Security (IPSec) and Secure Sockets Layer/Transport Layer Security (SSL/TLS) for protection of data in transit. IPSec is a protocol that extends the IP protocol stack, often in network infrastructure, and allows applications on upper layers to communicate securely without modification. SSL/TLS, on the other hand, operates at the session layer, and while there are third-party SSL/TLS wrappers, it often requires support at the application layer as well.

6.9.2 Business Associate Agreement

8.9.2 Describe whether or not it is willing to sign relevant and applicable Business Associate Agreement or any other agreement that may be necessary to protect data with a Purchasing Entity.

Armedia agrees and is willing to sign relevant and applicable Business Associate Agreements or any other agreement that may be necessary to protect data with a Purchasing Entity.

6.9.3 Data Usage

8.9.3 Offeror must describe how it will only use data for purposes defined in the Master Agreement, participating addendum, or related service level agreement. Offeror shall not use the government data or government related data for any other purpose including but not limited to data mining. Offeror or its subcontractors shall not resell nor otherwise redistribute information gained from its access to the data received as a result of this RFP.

Armedia does not access or use customer content for any purpose other than as legally required and to provide ArkCase SaaS services selected by each customer, to that customer and its end users. Armedia never uses customer content or derives information from it for other purposes such as marketing or advertising. Armedia will only use NASPO customer data for purposes defined in the Master Agreement, participating addendum, or related service level agreement. Armedia does not resell or redistribute customer information, and does not use customer information for data mining purposes.

6.10 Service Level Agreements

The ArkCase SaaS infrastructure is backed by the underlying AWS infrastructure on which it is built and thereby is supported by the AWS SLAs for its services.

Additionally, Armedia offers SLAs for ArkCase platform and its components. Please refer to information provided in section 6.10.2.

6.10.1 Negotiability

8.10.1 Offeror must describe whether your sample Service Level Agreement is negotiable. If not describe how it benefits purchasing entity's not to negotiate your Service Level Agreement.

Armedia provides the flexibility with our Service Level Agreement (SLA) to accommodate our customers' constraints.

6.10.2 Sample of a Service Level Agreement

8.10.2 Offeror, as part of its proposal, must provide a sample of its Service Level Agreement, which should define the performance and other operating parameters within which the infrastructure must operate to meet IT System and Purchasing Entity's requirements.

Service Level Agreement

Armedia's Service Level Agreement (SLA) makes Services available with a Monthly Uptime Percentage (defined below) of at least 99.9%, in each case during any monthly billing cycle (the "Service Commitment"). In the event Services do not meet the Service Commitment, the Purchasing Entity will be eligible to receive a Service Credit as described below. Armedia will issue a monthly report with Monthly Uptime Percentages and outlining issues or factors discussed in this SLA to provide greater understanding to the Purchasing Entity. ("SLA Reports")

Definitions

"**Monthly Uptime Percentage**" is calculated by subtracting from 100% the percentage of minutes during the month in which Services, as applicable, was in the state of "Region Unavailable" or "Unavailable". Monthly Uptime Percentage measurements exclude downtime resulting directly or indirectly from any Services SLA Exclusion (defined below).

"**Region Unavailable**" and "**Region Unavailability**" mean that more than one Availability Zone in which you are running an instance, within the same Region, is "**Unavailable**" to you.

"**Unavailable**" and "**Unavailability**" for Services is when all of your running instances have no external connectivity, or any material features of the Service are not operating in accordance with the Agreement, including the Response Time Commitment.

A "**Service Credit**" is a dollar credit, calculated as set forth below, that we may credit back to an eligible account.

Service Commitments and Service Credits

Service Credits are calculated as a percentage of the monthly charges paid by Purchasing Entity (excluding one-time payments) for Services (which were Unavailable) in the Region affected for the monthly billing cycle in which the Region Unavailability occurred in accordance with the schedule below.

Table 1 Monthly Uptime and Service Credit Percentage:

Monthly Uptime Percentage	Monthly Service Credit Percentage
Less than 98.0%	10%
Less than 95.0%	20%

We will apply any Service Credits only against future Services payments otherwise due from Purchasing Entity. A Service Credit will be applicable and issued only if the credit amount for the applicable monthly billing cycle is greater than one dollar ($1 USD). Service Credits may not be transferred or applied to any other account.

Credit Procedures

Armedia will issue Service Credits based on the SLA Reports on the next monthly invoice.

Armedia Services SLA Exclusions

The Service Commitment does not apply to any unavailability, suspension or termination of Services, or any other Services performance issues: (i) that result from a suspension of Services; (ii) caused by factors outside of our reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Services; (iii) that result from any actions or inactions of you or any third party; (iv) that result from your equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment, software or other technology within our direct control); (v) that result from failures of individual instances or volumes not attributable to Region Unavailability; (vi) that result from any maintenance as provided for pursuant to the Agreement; or (vii) arising from our `and

termination of your right to use Services in accordance with the Agreement (collectively, the "**Armedia Services SLA Exclusions**"). If availability is impacted by factors other than those used in our Monthly Uptime Percentage calculation, then we may issue a Service Credit considering such factors at our discretion.

Notifications

Armedia will develop a Communications Plan to govern the project; however, the table below defines the SLAs for notifying Purchasing Entity.

Table 2 Notifications

Incident Category	Notifier	Notification SLA to the Purchasing Entity	Notification SLA to Impacted Parties
Security breaches, compromise of PII data, and corruption of data	Armedia PM	Immediately and daily until a full understanding of the spillage and a consensus to stop reporting	Armedia will work with Purchasing Entity to draft a formal communication with the appropriate mitigations/remedies (i.e. credit monitoring)
Outages (RPO, RTO)	Armedia PM	Immediately and hourly until Services are operational	Immediately via website
Any other required notification	Armedia PM	As defined by the Communications Plan	As defined by the Communications Plan

Measuring SLA Performance

Armedia will provide a Service Report each month that identifies our adherence to the SLA. Each SLA criteria will be monitored and measured for compliance by Purchasing Entity.

SLA Enforcement Mechanisms

Armedia will provide a Service Report each month that identifies our adherence to the SLA. If Service Credits are warranted based on Table 1, Armedia will identify the Service Credits and how they will be applied to the next monthly invoice. If the Purchasing Entity disagrees with the Service Report, Armedia will work with the Purchasing Entity to come to consensus and apply the appropriate Service Credit if deem required.

Service Monitoring

Armedia will provide a Service Report each month that identifies our adherence to the SLA. Each SLA criteria will be monitored and measured daily of which the daily metrics will be compiled and presented in the report.

6.11 Data Disposal

8.11 Specify your data disposal procedures and policies and destruction confirmation process.

Armedia provides customers with the ability to delete their data. The Purchasing Entities retain control and ownership of their data, and it is the Purchasing Entity's responsibility to manage their data.

ACC uses AWS encrypted storage devices for storing the data and the data disposition during device decommissioning utilizes AWS data device decommissioning procedures that are designed to prevent customer data from being exAptOtaScEhmdEntOD unauthorized individuals. AWS uses the

techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.

6.12 Performance measures and Reporting

6.12.1 Reliability and Uptime

8.12.1 Describe your ability to guarantee reliability and uptime greater than 99.5%. Additional points will be awarded for 99.9% or greater availability.

Armedia offers a 99.9% availability of infrastructure for ArkCase SaaS. For applications developed by the Purchasing Entity using ADF, the reliability and uptime guarantee will need to be provided by the Purchasing Entity. Armedia is committed to supporting the Purchasing Entities for any issues with ADF pursuant to the terms of the purchased support service.

6.12.2 SLA Criteria

8.12.2 Provide your standard uptime service and related Service Level Agreement (SLA) criteria.

ArkCase infrastructure on ACC is backed by SLA guarantees of AWS on which it is based. AWS offers SLAs for services such as Amazon EC2 and Amazon EBS at 99.9%, and Amazon S3 with an SLA of 99.9%.

Armedia will provide a Service Report each month that identifies our adherence to the SLA. Each SLA criteria will be monitored and measured daily for which graphical reports will be presented to the Purchasing Entity and its customers.

6.12.3 End User Support

8.12.3 Specify and provide the process to be used for the participating entity to call/contact you for support, who will be providing the support, and describe the basis of availability.

The Armedia Customer Support Team will respond to tickets/requests 24 hours per day, 7 days a week (24x7). Table 3 defines severity class level response timeframes, effort required until resolution, and update frequencies currently employed by Armedia Customer Support Team:

Table 3 - Standard Support Response Time

Severity Class	Initial Response to Customer	Effort Required Until Resolution	Update Frequencies
Class 1	No greater than two hours if reported during normal business hours. Errors reported other times will receive a response on the next normal business day.	Constant effort during normal business hours until relief is provided in the form of a Work-Around or a software hotfix.	As mutually agreed but at a minimum, every business day during normal business hours via conference call or at Armedia's registered business location unless both Parties have agreed to a different frequency and location.
Class 2	Next business day but no greater than 24 hours.	Commercially reasonable efforts during normal business hours until there is a Work-Around or Call Remedy in the form of a software hotfix or service pack	As mutually agreed but at a minimum, Customer may request a summary report of all Severity 2 issues a maximum of once every five business days unless both Parties have agreed to a different frequency. Summary reports may be conveyed in e-mail format or verbally.
Class 3	No greater than five business days	Does not require immediate action. Normally addressed in a service pack at Armedia's sole discretion.	As mutually agreed but at a minimum, Customer may request a summary report of all Severity 3 issues a maximum of once per calendar month or per mutually agreed action plan.

Operations Management. The Armedia Operations Team will have a dedicated Project Manager who will oversee operational tasks such as system enhancements, problem resolution, change requests, system deployment and system performance inquiries.

Armedia will develop a Communications Plan to govern the project; however, **Error! Reference source not found.** defines the SLAs for notifying the Purchasing Entity and its customers

Table 4 Notifications

Incident Category	Point of Contact	Notification SLA to the <CUSTOMER>	Notification SLA to Impacted Parties
Security breaches, compromise of PII data, and corruption of data	Armedia PM	Immediately and daily until a full understanding of the spillage and a consensus to stop reporting	Armedia will work with <CUSTOMER> to draft a formal communication with the appropriate mitigations/remedies (i.e. credit monitoring)
Outages (RPO, RTO)	Armedia PM	Immediately and hourly until Services are operational	Immediately via website
Any other required notification	Armedia PM	As defined by the Communications Plan	As defined by the Communications Plan

6.12.4 SLA Remedies

8.12.4 Describe the consequences/SLA remedies if the Respondent fails to meet incident response time and incident fix time.

Service Credits are calculated as a percentage of the total charges paid by the Purchasing Entity and its customers and (excluding one-time payments) for Services (which were Unavailable) in

the Region affected for the monthly billing cycle in which the Region Unavailability occurred in accordance with the schedule below.

Table 5 - Monthly Uptime and Service Credit Percentage

Monthly Uptime Percentage	Monthly Service Credit Percentage
Less than 99.9%	10%
Less than 95.0%	20%

We will apply any Service Credits only against future Services payments otherwise due from the Purchasing Entity. A Service Credit will be applicable and issued only if the credit amount for the applicable monthly billing cycle is greater than one dollar ($1 USD). Service Credits may not be transferred or applied to any other account.

6.12.5 Planned Downtime Procedures

8.12.5 Describe the firm's procedures and schedules for any planned downtime.

ArkCase physical infrastructure on ACC does not require systems to be brought offline to perform regular maintenance and system patching, and AWS's own maintenance and system patching generally do not impact customers. There may be occasions when AWS might schedule a customer instance for a reboot for necessary maintenance, such as to apply updates that require a reboot. Armedia will communicate with the Purchasing Entity and its customers of any such known reboots. No action is required on the customer's part; we recommend that customers wait for the reboot to occur within its scheduled window. These scheduled events are not frequent and if a customer instance will be affected by a scheduled event, they will receive an email prior to the scheduled event with details about the event, as well as a start and end date. Customers can also view scheduled events for their instance(s) by using the Amazon EC2 Console, API, or CLI. AWS will communicate with customers, either via email, or through the AWS Service Health Dashboard if service use is likely to be adversely affected.

Besides these, the Purchasing Entities and their customers may incur a scheduled downtime for any application component upgrades on ACC. The Purchasing Entity would be responsible for such upgrades and its associated downtimes and would also be responsible in communicating that with their customers.

6.12.6 Disaster Recovery SLA Remedies

8.12.6 Describe the consequences/SLA remedies if disaster recovery metrics are not met.

Please refer to

SLA Remedies

6.12.7 Performance Reports

8.12.7 Provide a sample of performance reports and specify if they are available over the Web and if they are real-time statistics or batch statistics.
8.12.8 Ability to print historical, statistical, and usage reports locally.

Measuring SLA Performance

Armedia will provide a Service Report each month that identifies our adherence to the SLA. Each SLA criteria will be monitored and measured daily for which graphical reports will be presented to the Purchasing Entity and its customers. Purchasing Entities have the option of setting up role-based access controlled dynamic dashboards for real-time statistics (Figure 10).

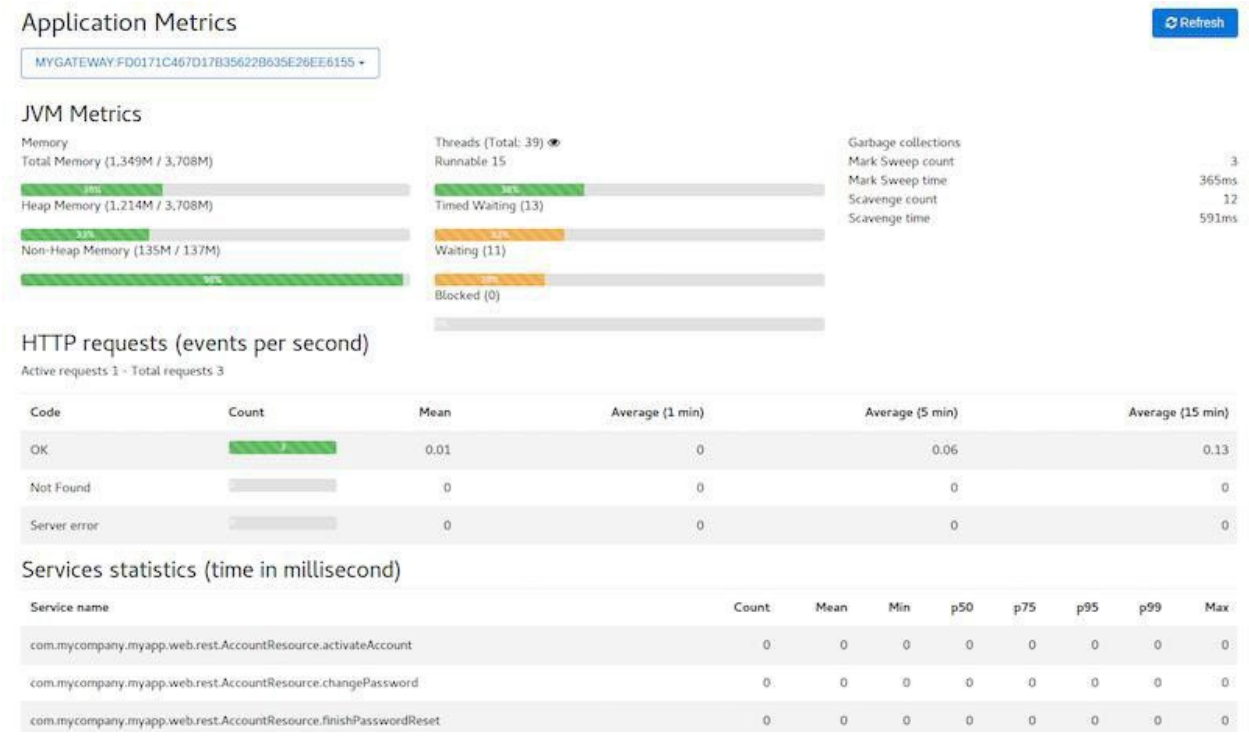


Figure 10 - ArkCase and ACC Key Performance Indicator Metrics Dashboard for real time statistics

SLA Enforcement Mechanisms

Armedia will provide a Service Report each month that identifies our adherence to the SLA. If Service Credits are warranted based on Table 5, Armedia will identify the Service Credits and how they will be applied to the next monthly invoice. If the Purchasing Entity disagrees with the Service Report, Armedia will work with the Purchasing Entity to come to consensus and apply the appropriate Service Credit if deem required.

Service Monitoring

Armedia will provide a Service Report each month that identifies our adherence to the SLA (Figure 11). Each SLA criteria will be monitored and measured daily of which the daily metrics will be compiled and presented in the report.

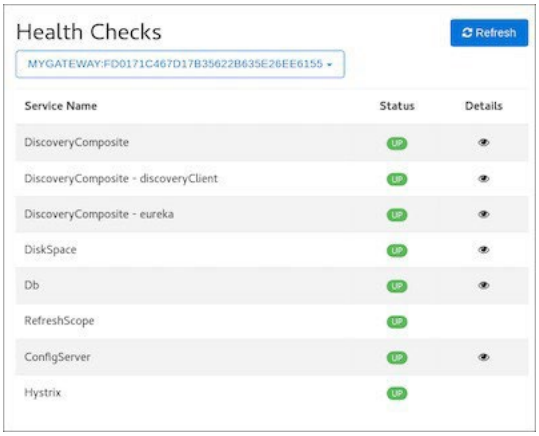


Figure 11 - ACC Health Check Dashboard for service monitoring

6.12.8 On-Demand Deployment and Scalability

8.12.9 Offeror must describe whether or not its on-demand deployment is supported 24x365.
8.12.10 Offeror must describe its scale-up and scale-down, and whether it is available 24x365.

ArkCase SaaS on ACC makes use of AWS auto scaling that allows the Purchasing Entities to automatically scale underlying resource capacity up or down according to conditions that they define (Figure 9). Auto Scaling is well suited for applications that experience hourly, daily, or weekly variability in usage. Customers can automatically scale their ACC fleet or maintain their ACC fleet at a set size.

Auto Scaling enables customers to closely follow the demand curve for their applications, reducing the need to provision ACC capacity for ArkCase SaaS in advance. For example, customers can set a condition to add new ACC instances in increments of three instances to the Auto Scaling Group when the average CPU utilization of the ACC fleet goes above 70%; and similarly, customers can set a condition to remove ACC instances in the same increments when CPU utilization falls below 10%.

Often, customers may want more time to allow their fleet to stabilize before Auto Scaling adds or removes more Amazon EC2 instances. Customers can configure a cool down period for their Auto Scaling Group, which tells Auto Scaling to wait for some time after taking an action before it evaluates the conditions again. Auto Scaling enables customers to run their Amazon EC2 fleet at optimal utilization.

Elastic Load Balancing

ArkCase SaaS on ACC also uses Elastic Load Balancing that automatically distributes incoming application traffic across multiple Amazon EC2 instances. It enables Purchasing Entity to achieve even greater fault tolerance in their applications, seamlessly providing the amount of load balancing capacity needed in response to incoming application traffic. Elastic Load Balancing detects unhealthy instances and automatically reroutes traffic to healthy instances until the unhealthy instances have been restored. Purchasing Entity can enable Elastic Load Balancing within a single Availability Zone or across multiple zones for even more consistent application performance (Figure 9).

6.13 Cloud Security Alliance

Describe and provide your level of disclosure with CSA Star Registry for each Solution offered.

a. Completion of a CSA STAR Self-Assessment. (3 points)
b. Completion of Exhibits 1 and 2 to Attachment B. (3 points)
c. Completion of a CSA STAR Attestation, Certification, or Assessment. (4 points)
d. Completion CSA STAR Continuous Monitoring. (5 points)

A CSA STAR Self-Assessment has been completed for Armedia's PaaS and SaaS offerings, and the CSA STAR CAIQ is attached. Please refer the response to section 8.6.2

6.14 Service Provisioning

6.14.1 Surge Support

8.14.1 Describe in detail how your firm processes emergency or rush services implementation requests by a Purchasing Entity.
8.14.2 Describe in detail the standard lead-time for provisioning your Solutions.

ArkCase SaaS on ACC uses AWS auto-scaling that provides the ability to scale computing resources up and down easily, with minimal friction. This elasticity helps you avoid provisioning resources up front for projects with variable consumption rates or short lifetimes. Instead of acquiring hardware, setting it up, and maintaining it in order to allocate resources to your applications, you use AWS to allocate resources using simple API calls. Elastic Load Balancing and Auto Scaling can automatically scale your AWS cloud-based resources up to meet unexpected demand, and then scale those resources down as demand decreases.

6.15 Back up and Disaster Plan

6.15.1 Legal Retention Periods

8.15.1 Ability to apply legal retention periods and disposition by agency per purchasing entity policy and/or legal requirements.

The Purchasing Entities control the entire life-cycle of their content on ArkCase SaaS and manage their content in accordance with their own specific needs, including content classification, access control, retention and deletion.

6.15.2 Mitigation Strategies

8.15.2 Describe any known inherent disaster recovery risks and provide potential mitigation strategies.

The ArkCase SaaS uses ACC infrastructure that has a high level of availability and we provide you with the features you need to deploy a resilient IT architecture. Our systems are designed to tolerate system or hardware failures with minimal customer impact. ArkCase SaaS on ACC supports many popular disaster recovery architectures, ranging from “pilot light” environments that are ready to scale up at a moment’s notice to “hot standby” environments that enable rapid failover.

All data centers are online and serving customers; no data center is “cold.” In the case of a failure, automated processes move your data traffic away from the affected area. By distributing applications across multiple AWS Availability Zones, you can remain resilient in the face of most failure modes, including natural disasters or system failures. You can build highly resilient systems in the cloud by employing multiple instances in multiple AWS Availability Zones and using data replication to achieve extremely high recovery time and recovery point objectives.

The Purchasing Entities are responsible for managing and testing the backup and recovery of their information system that is built on the ACC infrastructure. You can use the ACC infrastructure to enable faster disaster recovery of your critical IT systems without incurring the infrastructure expense of a second physical site.

6.15.4 The Support of Multiple Data Centers

8.15.3 Describe the infrastructure that supports multiple data centers within the United States, each of which supports redundancy, failover capability, and the ability to run large scale applications independently in case one data center is lost.

ArkCase SaaS on ACC relies on the AWS data centers for its infrastructure setup. The AWS Cloud infrastructure is built around regions and Availability Zones. A region is a physical location in the world where we have multiple Availability Zones. Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity and housed in separate facilities. These Availability Zones offer customers the ability to operate production applications and databases that are more highly available, fault tolerant, and scalable than would be possible with a single data center.

ArkCase SaaS on ACC can be setup using any combination of the AWS's 18 regions, 54 Availability Zones, and 1 Local Region throughout the world: US East (Northern Virginia), US East (Ohio), US West (Oregon), US West (Northern California), AWS GovCloud (US-West), Canada (Central), EU (Ireland), EU (Frankfurt), EU (London), EU (Paris), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), Asia Pacific (Seoul), Asia Pacific (Mumbai), Asia Pacific (Osaka-Local), South America (Sao Paulo), China (Beijing), and China (Ningxia).

6.16 5.16 Hosting and Provisioning

6.16.1 Cloud Hosting Provisioning Process

8.16.1 Documented cloud hosting provisioning processes, and your defined/standard cloud provisioning stack.

The ACC infrastructure for ArkCase SaaS can be controlled using the AWS Management Console which is a single destination for managing all AWS resources, from Amazon Elastic Compute Cloud (Amazon EC2) instances to Amazon DynamoDB tables. Purchasing Entities can use the AWS Management Console to perform any number of tasks, from deploying new applications to monitoring the health of applications. The AWS Management Console also enables customers to manage all aspects of their AWS account, including accessing monthly spending by service, managing security credentials, or even setting up new AWS Identity and Access Management (AWS IAM) users. The AWS Management Console supports all AWS Regions and lets customers provision resources across multiple regions.

6.16.2 Tool Sets

Provide tool sets at minimum for:
1. *Deploying new servers (determining configuration for both stand alone or part of an existing server farm, etc.)*
2. *Creating and storing server images for future multiple deployments*

The ACC for ArkCase SaaS uses the AWS management console to configure servers required for its business process automation offerings using ArkCase. ACC also uses a range of supporting components like management tools, networking services, and application augmentation services, with multiple interfaces to AWS Application Programming Interface (API)-based services, including Software Development Kits (SDKs), Integrated Development Environment (IDE) toolkits, and Command Line Tools.

3. Securing additional storage space

ACC for ArkCase SaaS uses AWS encrypted elastic block storage (EBS) and AWS elastic file system (EFS) for securely storing data. Amazon Elastic Block Store (Amazon EBS) provides block-level storage volumes for use with Amazon EC2 instances. Amazon EBS volumes are highly available and reliable storage volumes that can be attached to any running instance that is in the same Availability Zone. Amazon EBS volumes that are attached to an Amazon EC2 instance are exposed as storage volumes that persist independently from the life of the instance.

Amazon Elastic File System (Amazon EFS) provides simple, scalable file storage for use with Amazon EC2 instances in the AWS Cloud. Amazon EFS is easy to use and offers a simple interface that allows customers to create and configure file systems quickly and easily. With Amazon EFS, storage capacity is elastic, growing and shrinking automatically as files are added and removed, so applications have the storage they need, when they need it. Amazon EFS also allows customers to access file data from on-premises data centers. On-premises servers can move file data to and from an Amazon EFS file system when connected to an Amazon VPC with AWS Direct Connect, allowing customers to migrate data sets to Amazon EFS, enable cloud bursting scenarios, or back up on-premises data to Amazon EFS.

ArkCase SaaS uses AWS Import/Export Disk that accelerates moving large amounts of data into and out of the AWS cloud using portable storage devices for transport. AWS Import/Export Disk transfers data directly onto and off of storage devices using Amazon's high-speed internal network and bypassing the Internet. For significant data sets, AWS Import/Export Disk is often faster than Internet transfer and more cost effective than upgrading connectivity.

4. Monitoring tools for use by each jurisdiction's authorized personnel – and this should ideally cover components of a public (respondent hosted) or hybrid cloud (including Participating entity resources).

Monitoring of ACC for ArkCase SaaS is available for authorized personnel through the AWS management console which the Purchasing Entity can control through role-based access controls configured using the AWS identity management (IM).

6.17 Trial and Testing Periods (Pre- AND Post-Purchase)

6.17.1 Testing and Training Periods

8.17.1 Describe your testing and training periods that your offer for your service offerings.

Armedia uses test driven development for ArkCase as well as all the ADF services and components. The test results and the test coverage reports are published with every ADF release along with the release notes and are available to the Purchasing Entity.

6.17.2 Proof of Concept Environment

8.17.2 Describe how you intend to provide a test and/or proof of concept environment for evaluation that verifies your ability to meet mandatory requirements.

In collaboration with AWS, Armedia will provide test and proof of concept environments via Amazon Test Drive. Through Amazon Test Drive, Purchasing Entities will be able to spin up an environment and test drive the solution.

6.17.4 Training and Support

8.17.3 Offeror must describe what training and support it provides at no additional cost.

Armedia provides online training and videos at no additional cost via our website.

6.18 Integration and Customization

6.18.1 Integration

8.18.1 Describe how the Solutions you provide can be integrated to other complementary applications, and if you offer standard-based interface to enable additional integrations.

ArkCase uses a modular microservice-based architecture that uses REST APIs to loosely couple all the services (Figure 8). These REST APIs can be easily used to integrate with other complementary applications.

Based on the client demands, Armedia continuously researches and develops additional extension services for ArkCase using ADF that are available to customers as add-on options.

The ArkCase core platform is a Java/Spring framework-based application that ties together all the core services like document management, workflow management, security, auditing and reporting, etc., while providing a way to plug-in extension services through the micro-service architecture. **Optional** Service Extensions to ArkCase platform include, but are not limited to

- **Multi-factor authentication** (MFA) service extension developed for Pan-America Health Organization (PAHO) implementation ties the Okta multi-factor authentication platform into the ArkCase implementation for PAHO. This module also supports Ping MFA as an alternative. Additional MFA platform extensions can also be configured and supported through this extension.
- **Video/Audio transcription** service extension provides the ability to transcribe video and audio files to text and provide full text search capabilities on the video and audio files stored in the underlying content management system.
- **AWS Cloud service** extension adds the ability to make use of multiple AWS cloud services – the AWS transcription service being one of those. This adds the ability to use AWS storage (S3, Glacier) and AWS data analytics services as well as AWS data warehouse (RedShift) for the ArkCase platform as needed.
- **Advanced Data Analytics** extension allows ADF platform to use either the ElasticSearch-Logstash-Kibana (ELK) or the Solr-Logstash-Kibana (SiLK) platform stacks as the data analysis and visualization platform.

6.18.2 Customization

8.18.2 Describe the ways to customize and personalize the Solutions you provide to meet the needs of specific Purchasing Entities.

Purchasing Entities can follow the plug-n-play service architecture and develop customers' business logic as service extensions to the ArkCase platform using the ADF. This will enable the Purchasing Entity's customers to receive platform and component updates (updates for ArkCase core, Alfresco, Ephesoft etc.) without disrupting the business functionality of the customer.

5.19 MARKETING PLAN

Established in 2002 and operating out of Vienna, VA, Armedia, Inc. is a registered Veteran Owned Small Business and Minority Business Enterprise with verifiable success achieving more than $15M in annual revenue and consistent business growth. The company is building significant qualifications in Cloud Services, including a PaaS offering, the Armedia Development Framework. In addition, Armedia offers a comprehensive suite of information technology services to enhance its PaaS offering. These include ArkCase, a SaaS offering; deployment and migration services; data analytics; and technical advisory services to assist our customers in accessing the benefits of the Cloud. Shortly after Armedia was established, the company obtained subcontracts and prime contracts managing, securing, enhancing and optimizing numerous mission-critical applications for Federal agencies such as the Department of Justice (DoJ), Federal Bureau of Investigations (FBI), and commercial clients such as Delta Airlines and Purchasing Entity. Armedia continues to expand its service to the federal government providing cloud-centric services to the Postal Regulatory Commission (PRC), Pan American Health Organization (PAHO), and the US Department of Agriculture (USDA) Food and Nutrition Services (FNS). At the state and local level, Armedia provides IT support services, including cloud-oriented services, to Martin County in FL, Orange County FL, and New York State.

In 2012, Armedia was awarded a 5-year BPA by the USDA FNS for providing electronic content management services. Three years later, Armedia was awarded another 5-year BPA for six times the previous value, since that award we have introduced FNS to the Cloud, leveraging the Alfresco Content Management System and resulting in increased cost effectiveness and efficiency for their electronic content management. This contract has grown by $24.5M, which is a testament to the success that Armedia has been able to foster.

In 2017, the Pan-American Health Organization (PAHO) awarded a contract to Armedia to develop and implement a platform, the Regulatory Exchange Platform – secure (REPs), to facilitate the exchange of confidential/non-public information as well as the collaboration of global regulators in a secure IT environment. This is an international effort with initial participants including Australia, Brazil, Canada, Japan and the US. Additional countries are anticipated to join the effort soon. This platform will disseminate critical audit information on medical devices, enabling member countries to access inspection results with confidence and accuracy.

Armedia also won the contract to support the Postal Regulatory Commission (PRC) for the development of a cloud solution for their Electronic Document and Records Management System (EDRMS) which will be integrated with existing Commission systems such as email, intranet and extranet as well as replace the Commission's current Docket Management System (webDockets). PRC takes advantage of ArkCase's modular architecture which drives configuration versus customization, an important PRC requirement to avoid costly annual system upgrades and enhancements. Armedia's ArkCase serves as the basis for the PRC cloud solution (SaaS), hosted in AWS FedRAMP PaaS. In partnership with Armedia, PRC is the agency sponsor for Armedia to attain the FedRAMP Agency Path Authorization.

In addition to replacing PRC's legacy Docket Management System, Armedia will provide a Freedom of Information Act (FOIA) module in the next phase of the project, to be hosted on our FedRAMP PaaS.

Recognizing that the government's cloud market will be worth an estimated $28.85 Billion USD by 2022, Armedia is investing heavily in boAthttaictihsmPenataDS and SaaS cloud offerings through research

and development efforts, personnel training, partnerships development and marketing. Starting in 2015, the company developed an aggressive, multi-year growth plan, investing over $2M for this purpose. This initiative included hiring additional development personnel focused on R&D and cloud infrastructure, as well as expanding the dedicated business development division to bring in individuals tasked with marketing Armedia's services and capabilities to targeted audiences, and dedicated time and effort to the development of the cloud business at the state and federal government levels. Our team is multifunctional and includes delivery, operations and business development professionals; each providing guidance and advice in their particular areas of expertise. In support of this growth initiative, Armedia has invested in capture and proposal tools, enterprise infrastructure, digital marketing, brand awareness, and dedicated recruiting capability.

Situation Analysis

Armedia's Current Situation

Armedia developed the majority of its experience through prime awarded contracts on GSA Schedule 70 and on the open market. In addition, Armedia has been brought onto projects in a sub-contract arrangement by large systems integrators. Armedia continues to market aggressively to state businesses through its Schedule 70 GWAC and in open market solicitations. With the award of NASPO, Armedia will continue to market to our state business, recommending the use of the NASPO ValuePoint (NVP) Cloud Solution as a preferred avenue for placing business. We recognize that the NASPO Master Agreement offers strong value to state procurement initiatives in that it is flexible and efficient in terms of cost and time.

Market Trends

Government CIOs view the Cloud as a key practice to enable Information Technology to address the larger transformative shifts that are allowing them to better meet their agency's goals. Armedia has identified several market needs:

- Identifying challenges that government agencies face when procuring and adopting cloud technologies,
- Aligning FISMA and IT security with cloud-based hosting
- Assisting agencies in making the transition to a cloud-based environment
- Migration to the cloud-based services
- Legacy modernization, using cloud infrastructure

SWOT Analysis

Strengths

- Company's reputation and performance
- Long term clients and relationships
- Experienced professionals with federal, state and local government, and commercial experience
- Key government clients – USDA, DOD, Senate, FDA, PAHO and PRC
- Strong management emphasis on Cloud as a growth mechanism
- Continuous investing in R&D to enhance both the PaaS and SaaS offering
- Development in staff to support the growth goals through training and certifications indicating a long-term, strategic approach
- Investing in certifications such as CMMI Dev level 3 and ISO 9001.
- Competitive rates and low overhead contribute to a nimble approach toward our customers' needs
- Strong partnership with Amazon Web Services and currently on the Amazon MarketPlace.

Weaknesses

- Limited prime past performance at the state government level in offering Cloud Services specifically

Opportunities

- Expand footprint within state business by leveraging our current relationships built in the IT support services realms of ECM, Case Management and Records Management.
- Seek prime contracting opportunities with current customers and in our areas of expertise
- Cloud computing and IT modernization market is a fast growing area for the industry
- Corporate certifications in process (ISO 9001, CMMI Dev level 3, AWS)

Threats

- Highly competitive market
- Competitive labor market

Sales Strategies

Objectives

Growth

- Overall 5-year revenue growth – 35%
- New business – 30% of the revenue growth
- Maintain qualified BD pipeline that is continually evaluated and refreshed.
- 60% win rate
- Respond to RFIs in which we have strong qualifications and market toward the NASPO contract vehicle.
- Identify and pursue RFPs in our key capabilities areas, with states with whom we have a relationship, and that we have a strong probability to win.
- Develop relationships with additional states and their agencies through onsite visits, vendor outreach events and consistent contact management

Customer Development

- Develop a call plan for clients that revolves around their needs and the market
- Initial key states are Florida, New Hampshire, New York, and Virginia.
- Continually assess and adjust the plans to develop the relationship
- Build the relationship through visits, responding to RFIs and RFPs and establish a partnership orientation through providing thought leadership as the relationship progresses.

Pipeline Development

- Identify a short list of pre-RFP opportunities across key customers using a stringent qualification system
- Sources include GovWin, commercial databases, state acquisition forecasts, and personal visits with state representatives. Exercise a disciplined approach to determine each opportunity's qualitative and quantifiable value relevant to Armedia's business lines
- Classify each opportunity according to priority using a Salesforce based CRM
- Contact cognizant government and industry representatives for their perspectives on the relevant opportunities
- Conduct comprehensive competitive analysis, including competitor profiles, client's needs analysis and SWOT analysis relevant to the specific opportunity.

Action Plan for Success for NASPO ValuePoint (NVP) Cloud Solution

Action	Responsible Office
Develop growth plan	Business Development

Meet Stakeholders (internal) and educate them on NVP Cloud Solution	Management Team
Meet existing customers and educate them on NVP Cloud Solution, highlighting flexibility and ease of use of the vehicle.	Management Team
Develop Multi-year Pipeline of Qualified Opportunities	Business Development
Identify three new State agencies to target market	Business Development
Develop Industry call plan, including customer visits, tradeshows and conferences	Business Development
Market the NASPO ValuePoint Cloud Solution to state CPS's, staffers and potential using agencies	Business Development
Target state agencies with webinars and education sessions on current challenges that can be addressed through a cloud solution	Business Development

Resources Used in Developing Business

Dedicated Business Development Team	Conference attendance
Market Research Services, including Govwin, GovTribe, Bloomberg and FBO	Membership in key organizations, including Washington Technology, AFCEA and WIT
State Procurement Websites	Proposal consultants when needed
Salesforce CRM Platform	Dedicated Marketing Literature
Digital Marketing	Partnership Agreements
Branding	Vendor Outreach Sessions
Proposal Tools Update	PTAC and Agency specific Counseling Sessions

6.19 Related Value-Added Services to Cloud Solutions

8.20 Describe the valued-added services that you can provide as part of an awarded contract, e.g. consulting services pre- and post- implementation. Offerors may detail professional services in the RFP limited to assisting offering activities with initial setup, training and access to the services.

Besides providing ArkCase SaaS along with ADF for developing custom business process automation applications and ACC to deploy these applications, Armedia also provides full development support. The Purchasing Entity has the option to use Armedia's experienced development team to build custom solutions for their customers using ArkCase and ADF and deploying it on secure ACC infrastructure.

Armedia also has a team of AWS certified system engineers and developers that can work with the Purchasing Entity to help their customers with cloud adoption and cloud migration.

Armedia's advanced data analytics and machine learning division can help the Purchasing Entity develop solutions for their customers centered around data warehousing, data analysis, predictive analysis and machine learning using cloud services shown in Figure 12.

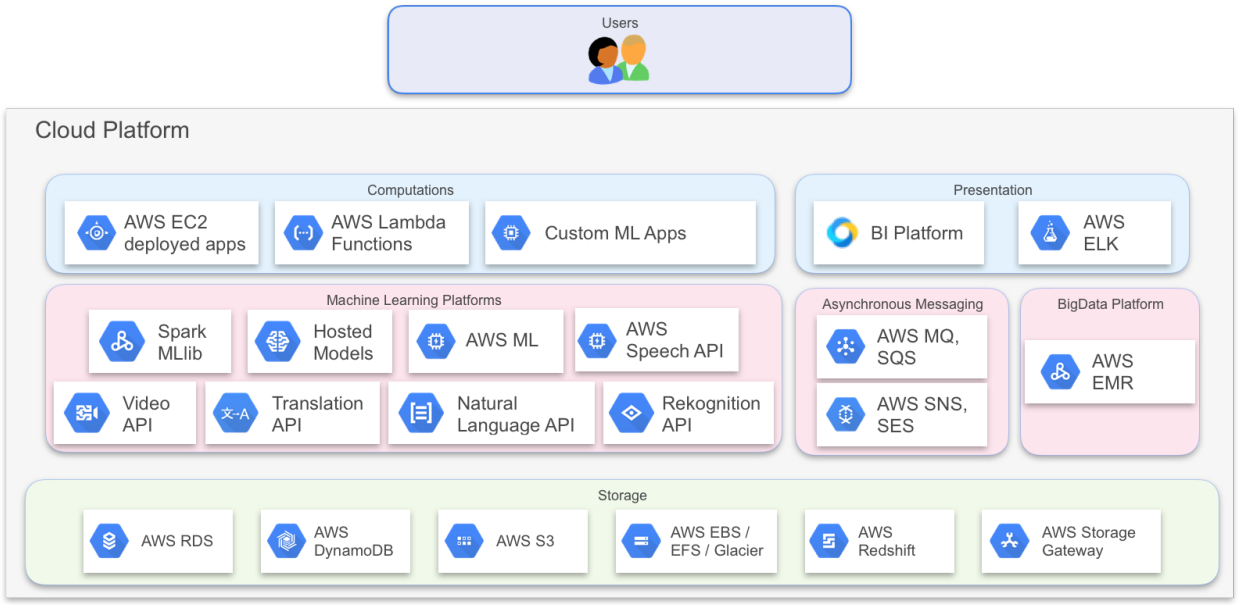


Figure 12 - Armedia's experience with cloud-based machine learning tools and solutions

6.20 Supporting Infrastructure

6.20.1 Infrastructure Needs

8.21.1 Describe what infrastructure is required by the Purchasing Entity to support your Solutions or deployment models.

ACC for ArkCase SaaS is designed to be auto-provisioned for ADF based solutions (Figure 9). Purchasing Entities have the option to provision additional resources and storage options based on their needs using the AWS management console.

6.20.2 Installation Needs

8.21.2 If required, who will be responsible for installation of new infrastructure and who will incur those costs?

ArkCase ships with support for containerized deployments using Kubernetes and Docker. The installation guide is provided along with ArkCase and ADF for custom installations as required.

Armedia's team of certified system engineers will work with the Purchasing Entity to help with the installation and setup of ArkCase based solutions when contracted.

APPENDIX A: ARKCASE VPAT

VPAT™
Voluntary Product Accessibility Template®
Version 1.3

The purpose of the **Voluntary Product Accessibility Template**, or **VPAT™**, is to assist Federal contracting officials and other buyers in making preliminary assessments regarding the availability of commercial "Electronic and Information Technology" products and services with features that support accessibility. It is assumed and recommended that offerors will provide additional contact information to facilitate more detailed inquiries.

The first table of the Template provides a summary view of the Section 508 Standards. The subsequent tables provide more detailed views of each subsection. There are three columns in each table. Column one of the Summary Table describes the subsections of subparts B and C of the Standards. The second column describes the supporting features of the product or refers you to the corresponding detailed table, e.g., "equivalent facilitation." The third column contains any additional remarks and explanations regarding the product. In the subsequent tables, the first column contains the lettered paragraphs of the subsections. The second column describes the supporting features of the product with regard to that paragraph. The third column contains any additional remarks and explanations regarding the product.

Date: 7/6/18
Name of Product: ArkCase
Contact for more Information (name/phone/email): James Bailey / (571) 261-8640 / james.bailey@armedia.com

Summary Table
VPAT™
Voluntary Product Accessibility Template®

Criteria	**Supporting Features**	**Remarks and explanations**
Section 1194.21 Software Applications and Operating Systems		
Section 1194.22 Web-based Internet Information and Applications		
Section 1194.23 Telecommunications Products		
Section 1194.24 Video and Multi-media Products		
Section 1194.25 Self-Contained, Closed Products		
Section 1194.26 Desktop and Portable Computers		

Section 1194.31 Functional Performance Criteria		
Section 1194.41 Information, Documentation and Support		

Section 1194.21 Software Applications and Operating Systems – Detail
VPAT™
Voluntary Product Accessibility Template®

Criteria	**Supporting Features**	**Remarks and explanations**
(a) When software is designed to run on a system that has a keyboard, product functions shall be executable from a keyboard where the function itself or the result of performing a function can be discerned textually.	Supported	Use of the tab key and enter keys are fully operational.
(b) Applications shall not disrupt or disable activated features of other products that are identified as accessibility features, where those features are developed and documented according to industry standards. Applications also shall not disrupt or disable activated features of any operating system that are identified as accessibility features where the application programming interface for those accessibility features has been documented by the manufacturer of the operating system and is available to the product developer.	Supported	ArkCase does not require nor does it impair any 3rd party applications. It is written on web-based standards.
(c) A well-defined on-screen indication of the current focus shall be provided that moves among interactive interface elements as the input focus changes. The focus shall be programmatically exposed so that Assistive Technology can track focus and focus changes.	Supported	We use HOVER and ACTIVE states on all of our HTML objects as well as input boxes when they are active.
(d) Sufficient information about a user interface element including the identity, operation and state of the element shall be available to Assistive Technology. When an image represents a program element, the information conveyed by the image must also be available in text.	Supported	All images are rendered using CSS with a text-equivalent in HTML.

(e) When bitmap images are used to identify controls, status indicators, or other programmatic elements, the meaning assigned to those images shall be consistent throughout an application's performance.	Supported	We are very consistent with our use of graphics.
(f) Textual information shall be provided through operating system functions for displaying text. The minimum information that shall be made available is text content, text input caret location, and text attributes.	Supported	The minimal information is available as text.
(g) Applications shall not override user selected contrast and color selections and other individual display attributes.	Supported	ArkCase does not override the system's contrast and display attributes.
(h) When animation is displayed, the information shall be displayable in at least one non-animated presentation mode at the option of the user.	Supported	The only animations we use are for a "loading" indication. The ALT tag on that image is "Loading. Please wait for the results to load."
(i) Color coding shall not be used as the only means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.	Supported	We use color, the use of STRONG and EM tags, and the use of H1-H6 tags to indicate information. We also use the LABEL attribute to indicate a form field title.
(j) When a product permits a user to adjust color and contrast settings, a variety of color selections capable of producing a range of contrast levels shall be provided.	N/A	Our product does not allow the user to adjust the color or contrast settings.
(k) Software shall not use flashing or blinking text, objects, or other elements having a flash or blink frequency greater than 2 Hz and lower than 55 Hz.	N/A	We do not use flashing or blinking text.
(l) When electronic forms are used, the form shall allow people using Assistive Technology to access the information, field elements, and functionality required for completion and submission of the form, including all directions and cues.	Supported	Our electronic forms support assistive technology in all of these ways.

Section 1194.22 Web-based Internet information and applications – Detail
VPAT™
Voluntary Product Accessibility Template®

Criteria	**Supporting Features**	**Remarks and explanations**
(a) A text equivalent for every non-text element shall be provided (e.g., via "alt", "longdesc", or in element content).	Supported	We do provide text equivalents everywhere.
(b) Equivalent alternatives for any multimedia presentation shall be synchronized with the presentation.	Supported	We do provide text equivalents for media, but a user must enable the accessibility setting if they choose to add a document as a PDF.
(c) Web pages shall be designed so that all information conveyed with color is also available without color, for example from context or markup.	Supported	We use emphasis tags such as STRONG and EM as well as color to convey information.
(d) Documents shall be organized so they are readable without requiring an associated style sheet.	Supported	The application is readable, although not very user friendly, without the user of a style sheet.
(e) Redundant text links shall be provided for each active region of a server-side image map.	Supported	We do not use image maps.
(f) Client-side image maps shall be provided instead of server-side image maps except where the regions cannot be defined with an available geometric shape.	Supported	We do not use image maps.
(g) Row and column headers shall be identified for data tables.	Supported	We do use table headers, footers, and caption tags to describe the tables appropriately.
(h) Markup shall be used to associate data cells and header cells for data tables that have two or more logical levels of row or column headers.	Supported	We do associate our cells with our headers for easy tabbing using assistive technology.
(i) Frames shall be titled with text that facilitates frame identification and navigation	Supported	We do not use frames.

(j) Pages shall be designed to avoid causing the screen to flicker with a frequency greater than 2 Hz and lower than 55 Hz.	Supported	We do not use a flicker or animation.
(k) A text-only page, with equivalent information or functionality, shall be provided to make a web site comply with the provisions of this part, when compliance cannot be accomplished in any other way. The content of the text-only page shall be updated whenever the primary page changes.	Not Applicable	We do not provide a text-only version of the application because our product is already accessible.
(l) When pages utilize scripting languages to display content, or to create interface elements, the information provided by the script shall be identified with functional text that can be read by Assistive Technology.	Supported	We do our best to let the user know when content been changed and assistive technology will help the user do that.
(m) When a web page requires that an applet, plug-in or other application be present on the client system to interpret page content, the page must provide a link to a plug-in or applet that complies with §1194.21(a) through (l).	Supported	When 3rd party plugins are used, we provide a link to the plug-in for the user to download.
(n) When electronic forms are designed to be completed on-line, the form shall allow people using Assistive Technology to access the information, field elements, and functionality required for completion and submission of the form, including all directions and cues.	Supported	We do support this.
(o) A method shall be provided that permits users to skip repetitive navigation links.	Supported	We support this.
(p) When a timed response is required, the user shall be alerted and given sufficient time to indicate more time is required.	Supported	We do have a timeout that the user is alerted to and they'r egiven the option to extend their session.

Note to 1194.22: The Board interprets paragraphs (a) through (k) of this section as consistent with the following priority 1 Checkpoints of the Web Content Accessibility Guidelines 1.0 (WCAG 1.0) (May 5 1999) published by the Web Accessibility Initiative of the World Wide Web Consortium: Paragraph (a) - 1.1, (b) - 1.4, (c) - 2.1, (d) - 6.1, (e) - 1.2, (f) - 9.1, (g) - 5.1, (h) - 5.2, (i) - 12.1, (j) - 7.1, (k) - 11.4.

Section 1194.23 Telecommunications Products – Detail
VPAT™
Voluntary Product Accessibility Template®

Criteria	**Supporting Features**	**Remarks and explanations**
(a) Telecommunications products or systems which provide a function allowing voice communication and which do not themselves provide a TTY functionality shall provide a standard non-acoustic connection point for TTYs. Microphones shall be capable of being turned on and off to allow the user to intermix speech with TTY use.	N/A	
(b) Telecommunications products which include voice communication functionality shall support all commonly used cross-manufacturer non-proprietary standard TTY signal protocols.	N/A	
(c) Voice mail, auto-attendant, and interactive voice response telecommunications systems shall be usable by TTY users with their TTYs.	N/A	
(d) Voice mail, messaging, auto-attendant, and interactive voice response telecommunications systems that require a response from a user within a time interval, shall give an alert when the time interval is about to run out, and shall provide sufficient time for the user to indicate more time is required.	N/A	
(e) Where provided, caller identification and similar telecommunications functions shall also be available for users of TTYs, and for users who cannot see displays.	N/A	
(f) For transmitted voice signals, telecommunications products shall provide a gain adjustable up to a minimum of 20 dB. For incremental volume control, at least one intermediate step of 12 dB of gain shall be provided.	N/A	
(g) If the telecommunications product allows a user to adjust the receive	N/A	

volume, a function shall be provided to automatically reset the volume to the default level after every use.		
(h) Where a telecommunications product delivers output by an audio transducer which is normally held up to the ear, a means for effective magnetic wireless coupling to hearing technologies shall be provided.	N/A	
(i) Interference to hearing technologies (including hearing aids, cochlear implants, and assistive listening devices) shall be reduced to the lowest possible level that allows a user of hearing technologies to utilize the telecommunications product.	N/A	
(j) Products that transmit or conduct information or communication, shall pass through cross-manufacturer, non-proprietary, industry-standard codes, translation protocols, formats or other information necessary to provide the information or communication in a usable format. Technologies which use encoding, signal compression, format transformation, or similar techniques shall not remove information needed for access or shall restore it upon delivery.	N/A	
(k)(1) Products which have mechanically operated controls or keys shall comply with the following: Controls and Keys shall be tactilely discernible without activating the controls or keys.	N/A	
(k)(2) Products which have mechanically operated controls or keys shall comply with the following: Controls and Keys shall be operable with one hand and shall not require tight grasping, pinching, twisting of the wrist. The force required to activate controls and keys shall be 5 lbs. (22.2N) maximum.	N/A	
(k)(3) Products which have mechanically operated controls or keys shall comply with the following: If key repeat is supported, the delay before repeat shall be adjustable to at least 2 seconds. Key	N/A	

repeat rate shall be adjustable to 2 seconds per character.		
(k)(4) Products which have mechanically operated controls or keys shall comply with the following: The status of all locking or toggle controls or keys shall be visually discernible, and discernible either through touch or sound.	N/A	

Section 1194.24 Video and Multi-media Products – Detail
VPAT™
Voluntary Product Accessibility Template®

Criteria	**Supporting Features**	**Remarks and explanations**
a) All analog television displays 13 inches and larger, and computer equipment that includes analog television receiver or display circuitry, shall be equipped with caption decoder circuitry which appropriately receives, decodes, and displays closed captions from broadcast, cable, videotape, and DVD signals. As soon as practicable, but not later than July 1, 2002, widescreen digital television (DTV) displays measuring at least 7.8 inches vertically, DTV sets with conventional displays measuring at least 13 inches vertically, and stand-alone DTV tuners, whether or not they are marketed with display screens, and computer equipment that includes DTV receiver or display circuitry, shall be equipped with caption decoder circuitry which appropriately receives, decodes, and displays closed captions from broadcast, cable, videotape, and DVD signals.	N/A	
(b) Television tuners, including tuner cards for use in computers, shall be equipped with secondary audio program playback circuitry.	N/A	
(c) All training and informational video and multimedia productions which support the agency's mission, regardless of format, that contain speech or other audio information	N/A	

necessary for the comprehension of the content, shall be open or closed captioned.		
(d) All training and informational video and multimedia productions which support the agency's mission, regardless of format, that contain visual information necessary for the comprehension of the content, shall be audio described.	N/A	
(e) Display or presentation of alternate text presentation or audio descriptions shall be user-selectable unless permanent.	N/A	

Section 1194.25 Self-Contained, Closed Products – Detail
VPAT™
Voluntary Product Accessibility Template®

Criteria	**Supporting Features**	**Remarks and explanations**
(a) Self contained products shall be usable by people with disabilities without requiring an end-user to attach Assistive Technology to the product. Personal headsets for private listening are not Assistive Technology.	N/A	
(b) When a timed response is required, the user shall be alerted and given sufficient time to indicate more time is required.	N/A	
(c) Where a product utilizes touchscreens or contact-sensitive controls, an input method shall be provided that complies with §1194.23 (k) (1) through (4).	N/A	
(d) When biometric forms of user identification or control are used, an alternative form of identification or activation, which does not require the user to possess particular biological characteristics, shall also be provided.	N/A	
(e) When products provide auditory output, the audio signal shall be provided at a standard signal level through an industry standard connector that will allow for private listening. The product must provide the ability to interrupt, pause, and restart the audio at anytime.	N/A	

(f) When products deliver voice output in a public area, incremental volume control shall be provided with output amplification up to a level of at least 65 dB. Where the ambient noise level of the environment is above 45 dB, a volume gain of at least 20 dB above the ambient level shall be user selectable. A function shall be provided to automatically reset the volume to the default level after every use.	N/A	
(g) Color coding shall not be used as the only means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.	N/A	
(h) When a product permits a user to adjust color and contrast settings, a range of color selections capable of producing a variety of contrast levels shall be provided.	N/A	
(i) Products shall be designed to avoid causing the screen to flicker with a frequency greater than 2 Hz and lower than 55 Hz.	N/A	
(j) (1) Products which are freestanding, non-portable, and intended to be used in one location and which have operable controls shall comply with the following: The position of any operable control shall be determined with respect to a vertical plane, which is 48 inches in length, centered on the operable control, and at the maximum protrusion of the product within the 48 inch length on products which are freestanding, non-portable, and intended to be used in one location and which have operable controls.	N/A	
(j)(2) Products which are freestanding, non-portable, and intended to be used in one location and which have operable controls shall comply with the following: Where any operable control is 10 inches or less behind the reference plane, the height shall be 54 inches maximum and 15 inches minimum above the floor.	N/A	
(j)(3) Products which are freestanding, non-portable, and intended to be used in one location and which have operable	N/A	

controls shall comply with the following: Where any operable control is more than 10 inches and not more than 24 inches behind the reference plane, the height shall be 46 inches maximum and 15 inches minimum above the floor.		
(j)(4) Products which are freestanding, non-portable, and intended to be used in one location and which have operable controls shall comply with the following: Operable controls shall not be more than 24 inches behind the reference plane.	N/A	

Section 1194.26 Desktop and Portable Computers – Detail
VPAT™
Voluntary Product Accessibility Template®

Criteria	**Supporting Features**	**Remarks and explanations**
(a) All mechanically operated controls and keys shall comply with §1194.23 (k) (1) through (4).	N/A	
(b) If a product utilizes touchscreens or touch-operated controls, an input method shall be provided that complies with §1194.23 (k) (1) through (4).	N/A	
(c) When biometric forms of user identification or control are used, an alternative form of identification or activation, which does not require the user to possess particular biological characteristics, shall also be provided.	N/A	
(d) Where provided, at least one of each type of expansion slots, ports and connectors shall comply with publicly available industry standards	N/A	

Section 1194.31 Functional Performance Criteria – Detail
VPAT™
Voluntary Product Accessibility Template®

Criteria	**Supporting Features**	**Remarks and explanations**
(a) At least one mode of operation and information retrieval that does not require user vision shall be provided, or support for Assistive Technology used by people who are blind or visually impaired shall be provided.	N/A	
(b) At least one mode of operation and information retrieval that does not require visual acuity greater than 20/70 shall be provided in audio and enlarged print output working together or independently, or support for Assistive Technology used by people who are visually impaired shall be provided.	N/A	
(c) At least one mode of operation and information retrieval that does not require user hearing shall be provided, or support for Assistive Technology used by people who are deaf or hard of hearing shall be provided	N/A	
(d) Where audio information is important for the use of a product, at least one mode of operation and information retrieval shall be provided in an enhanced auditory fashion, or support for assistive hearing devices shall be provided.	N/A	
(e) At least one mode of operation and information retrieval that does not require user speech shall be provided, or support for Assistive Technology used by people with disabilities shall be provided.	N/A	
(f) At least one mode of operation and information retrieval that does not require fine motor control or simultaneous actions and that is operable with limited reach and strength shall be provided.	N/A	

Section 1194.41 Information, Documentation and Support – Detail
VPAT™
Voluntary Product Accessibility Template®

Criteria	**Supporting Features**	**Remarks and explanations**
(a) Product support documentation provided to end-users shall be made available in alternate formats upon request, at no additional charge	Not Supported	Needs further investigation.
(b) End-users shall have access to a description of the accessibility and compatibility features of products in alternate formats or alternate methods upon request, at no additional charge.	Not Supported	Needs further investigation.
(c) Support services for products shall accommodate the communication needs of end-users with disabilities.	Not Supported	Needs further investigation.

The State of Utah
Division of Purchasing
In conjunction with

Response to:
Utah Solicitation Number SK18008

NASPO ValuePoint
NASPO ValuePoint Master Agreement for Cloud Solutions
Technical Response Platform as a Service (PaaS)

Submitted by:

Armedia, LLC
8221 Old Courthouse Road
Suite 300
Vienna, VA 22182
www.armedia.com

CMMI Level 3 Appraised
Veteran Owned Small Business (VOSB)
TIN30-0067329
DUNS – 133097183
CAGE/NCAGE Code – 3HAW7
GSA IT70 - GS35F0891P

Submitted to:

Mr. Solomon Kingston
State Contract Analyst
State of Utah, Division of Purchasing
skingston@utah.gov
(801)538 - 3228

Table of Contents

6 TECHNICAL RESPONSE

A specific point-by-point response, in the order listed, to each requirement in the Section 8 of the RFP.

Armedia is an Amazon Web Service (AWS) Consulting partner specializing in building PaaS and SaaS solutions using cloud technologies and infrastructure. We specialize in building cost-effective, secure and scalable cloud-based solutions in the areas of content management, data analytics, system usage and behavior analysis, machine learning and business process automations.

With our staff of certified cloud engineers and solution developers, Armedia is well suited to support NASPO's Purchasing Entities with their cloud migration and cloud adoptions through SaaS and PaaS implementations.

Armedia Content Cloud (ACC)

Armedia realizes that each organization needs differ from one another and in many instances, a COTS product may not be able to satisfy all the requirements of the organization. For such instances, Armedia offers Armedia Content Cloud (ACC - Figure 1) – an operational and fully provisioned infrastructure that meets FedRAMP moderate requirement out-of-the-box – as a platform for the organization to build custom solutions in the areas of:

- Content, Document and Information Management
- Records Management
- Workflows, Business Process Automation and Case Management
- Business Intelligence and Reporting
- E-Discovery, Research and Collaboration
- Business Rules and Policy Management
- Data Analysis including Taxonomy and Semantic Analysis
- Security and Access Controls

As a platform as a service (PaaS) offering, the authorized ACC system allows customers to meet agency requirements without major capital investment and with reduced technical staff. Armedia provides full, professional management of the PaaS offering, and the infrastructure supporting the PaaS includes professionally hosted servers, storage, network connectivity, and associated management systems. ACC offers a suite of three SaaS solutions -- the ArkCase case management system, the Alfresco enterprise content management (ECM) system and the Ephesoft Intelligent Document Capture system along with Pentaho for Business Intelligence and Reporting and Solr for full text search and indexing.

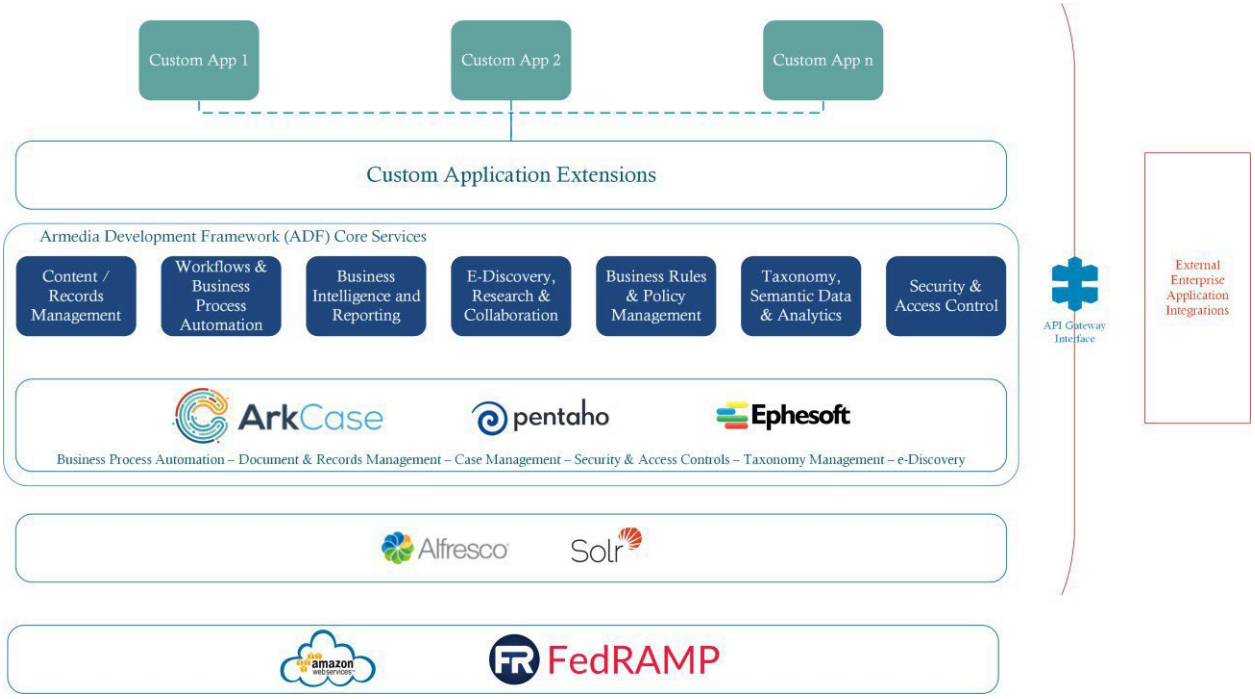


Figure 1 - Armedia Content Cloud for building and deploying custom applications for consumers

Armedia Development Framework (ADF)

Armedia also offers the Armedia Development Framework (ADF) that extends the ACC offering and provides a Java based application development framework that includes additional services and platform integration which may or may not be FedRAMP ready. The customer – based on the specific requirements – can choose to use these services along with the basic ACC offerings and create custom applications using standard J2EE/Spring framework, Spring REST and Angular. The development framework (depicted in *Figure 2 - Armedia Development Framework Services and Extensions*) is an accelerator offered by Armedia for custom cloud-based application development in the areas of Content and Information Management and Data Analysis.

The ADF ships with containerized deployment modules based on Docker and Kubernetes along with Ansible integration for orchestrating the deployment, installation and setup of the custom application and all its components on any cloud environments.

Figure 2 - Armedia Development Framework Services and Extensions – Framework to create custom applications extending the ACC offerings

Armedia provides application modernization services based on the ADF that enable NASPO's Purchasing Entities to offer cloud-based solutions along with cloud migration and cloud adoption strategies to its customers.

At its core, the ADF is a modular microservice-based application development framework based on Java and Spring Framework components that integrate different core application components like ArkCase – Armedia's SaaS offering for business process automation and case management, Alfresco ECM, a relational database, Pentaho BI platform, ElasticSearch-Logstash-Kibana (ELK), etc. and provide REST based API extensions to the underlying services. The underlying components like Alfresco, Pentaho, ELK, etc. can be swapped for an equivalent tool if any such tool already exists with the Purchasing Entity's customer.

ADF employs a modern microservice-based architecture that is flexible and scalable to handle huge volumes of data and high number of user interactions.

Figure 2 depicts the technology stack used in the ADF. The ADF core is a Java/Spring framework-based application that ties together all the core services like document management, workflow management, security, auditing and reporting, etc., while providing a way to plug-in extension services through the micro-service architecture. **Optional** Service Extensions to the ADF platform include, but are not limited to

- **Multi-factor authentication** (MFA) service extension developed for Pan-America Health Organization (PAHO) implementation ties the Okta multi-factor authentication platform into the ArkCase implementation for PAHO. This module also supports Ping MFA as an alternative. Additional MFA platform extensions can also be configured and supported through this extension.
- **Video/Audio transcription** service extension provides the ability to transcribe video and audio files to text and provide full text search capabilities on the video and audio files stored in the underlying content management system.
- **AWS Cloud service** extension adds the ability to make use of multiple AWS cloud services – the AWS transcription service being one of those. This adds the ability to use AWS storage (S3, Glacier) and AWS data analytics services as well as AWS data warehouse (RedShift) for the ArkCase platform as needed.
- **Advanced Data Analytics** extension allows ADF platform to use either the ElasticSearch-Logstash-Kibana (ELK) or the Solr-Logstash-Kibana (SiLK) platform stacks as the data analysis and visualization platform.

Following the same plug-n-play service architecture, the Purchasing Entity's customers' business logic will be built using ADF as service extensions to the platform. This will enable the Purchasing Entity's customers to receive platform and component updates (updates for ArkCase core, Alfresco, Activiti etc.) without disrupting the business functionality of the customer.

6.1 Technical Requirements

6.1.1 NIST

8.1.1 For the purposes of the RFP, meeting the NIST essential characteristics is a primary concern. As such, describe how your proposed solution(s) meet the characteristics defined in NIST Special Publication 800-145.

Armedia's PaaS and SaaS offerings are designed and operated as cloud-based services, as defined in NIST Special Publication 800-145 – see the response to sections 8.1.2 and 8.1.3. In addition, Armedia follows applicable information security controls for a Moderate impact system from NIST Special Publication 800-53 as a configuration, architectural, and operational baseline.

The National Institute of Standards and Technology (NIST) 800-53 Rev. 4 security controls are generally applicable to Federal Information Systems. These are typically systems that must go through a formal assessment and authorization process to ensure sufficient protection of confidentiality, integrity, and availability of information and information systems, based on the security category and impact level of the system (low, moderate, or high), and a risk determination.

Armedia has standardized on FedRAMP as the common security framework which is based on the NIST 800-53 Rev. 4 security controls, and has extra requirements based on the impact levels for cloud applications built using ADF as PaaS and deployed on ACC. Armedia has elected to abide by the Moderate impact level. In order to obtain FedRAMP accreditation, a Third-Party Assessment Organization (3PAO) must be engaged to audit the System Security Plan (SSP). The 3PAO will review the policies and procedures as well as verify evidence the organization is following the controls and practices. Many of the FedRAMP controls overlap HIPAA's security rules. NIST's 800-66 publication documents the alignment of the NIST 800-53 controls used by FedRAMP and HIPAA's security rules.

Armedia's ACC and ADF PaaS relies on AWS' NIST-compliant cloud infrastructure services that have been validated by third-party testing performed against the NIST 800-53 Rev. 4 controls plus FedRAMP requirements. AWS has received FedRAMP Authorizations to Operate (ATO) from multiple authorizing agencies for both the AWS GovCloud (US) Region and the AWS US East/West regions.

6.1.2 Requirements of Attachments C & D

*8.1.2 As applicable to an Offeror's proposal, Offeror must describe its willingness to comply with, the requirements of **Attachments C & D**.*

Visibility to Purchasing Entities:
Armedia offers ACC and ADF as PaaS – a development platform that uses ArkCase for custom application development and deployment allowing the Purchasing Entity to develop various business process automation solutions along with Document and Information Management, Records Management, Data Analytics and Visualization components for their customers.

Primary Focus of the Service:
ACC and ADF are primarily focused on PaaS model.

Purchasing Entity Role:
Purchasing Entity can develop custom applications using ADF components that will enable them to provide customized applications to their customers that can include:

- Document Management
- Records Management
- Case Management
- Compliance Management
- Complaints Management
- License and Permits Management
- Customer Relationship Management
- Data Analytics
- E-Discovery
- Business Intelligence and Reporting

ADF enables purchasing entities to create their own versions of SaaS packages that can be offered to their customers.

Lowest Level of Configurability:
The lowest level of configurability for out-of-the-box implementation of ArkCase is as PaaS.

6.1.3 Offerings identified in Scope of Services

*8.1.3 As applicable to an Offeror's proposal, Offeror must describe how its offerings adhere to the services, definitions, and deployment models identified in the Scope of Services, in **Attachment D**.*

Categorization of Risk

ACC is designed to handle Moderate and Low Risk Data with emphasis on data security. ACC follows FedRAMP's requirements for a Moderate classification on its operations and uses NIST 800-53 for the baseline security controls. Following NIST's 800-53 controls allows ArkCase to meet HIPAA requirements (see NIST's 800-66 which provides the alignment of NIST 800-53 and HIPAA Security rules). ACC uses AWS's EBS encryption to encrypt data at rest and all snapshots created from the volume. Volumes are encrypted using AES-256 by AWS's Key Management Service (KMS). By default, Armedia uses AWS's KMS to create, manage, and rotate keys. An option exists to import existing keys owned by NASPO's Purchasing Entities if required. All data is encrypted in transit using TLS 1.1 or 1.2. This includes communications from the Internet into the entry point of the system, as well as internal communications (web servers to application servers, application servers to databases, all directory services, monitoring traffic, etc.).

AWS Key Management Service provides centralized control over the encryption keys used to protect data. Armedia will work with NASPO's Purchasing Entities to create, import, rotate, disable, delete, define usage policies for, and audit the use of encryption keys used to encrypt data. AWS Key Management Service is integrated with several other AWS services making it easy to encrypt the data stored in services with encryption keys you control. AWS KMS is integrated with AWS CloudTrail which provides you the ability to audit who used which keys, on which resources, and when.

Service & Models

The NIST definition lists five essential characteristics of cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion, and measured service. The definition is intended to serve as a means for broad comparisons of cloud services and deployment strategies, and to provide a baseline for discussion from what is cloud computing to how to best use cloud computing. The following sections detail how AWS meets the NIST definition of cloud.

On-Demand Self-Service

Armedia's ACC is built on AWS cloud services adding and deploying the basic tools for building business process automation solutions centered around ArkCase and ADF. AWS provides customers of all sizes with on-demand access to a wide range of cloud infrastructure services, charging you only for the resources you actually use. AWS enables you to eliminate the need for costly hardware and the administrative pain that goes along with owning and operating it. Instead of the weeks and months it takes to plan, budget, procure, set up, deploy, operate, and hire for a new project, our customers can simply sign up for AWS and immediately begin deployment in the cloud with the equivalent of 1, 10, 100, or 1,000 servers. Whether an organization needs to prototype an application or host a production solution, AWS makes it simple for customers to get started and be productive.

Broad Network Access

Armedia's ACC leverages AWS resources and storage options and provides a simple way to access servers, storage, databases, and a broad set of application services over the Internet. Cloud computing providers such as AWS own and maintain the network-connected hardware required for these application services, while you provision and use what you need via a web application.

Resource Pooling

The ACC environment is a virtualized, multi-tenant environment. ACC uses and builds upon the AWS implemented security management processes, PCI controls, and other security controls designed to isolate each customer from other customers. AWS systems are designed to prevent customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software. This architecture has been validated by an independent PCI Qualified Security Assessor (QSA) and was found to be in compliance with all requirements of PCI DSS Security Standards 3.2 as of July 2016.

Rapid Elasticity

ACC relies on AWS that provides a massive global cloud infrastructure that allows you to quickly innovate, experiment, and iterate. Instead of waiting weeks or months for hardware, you can instantly deploy new applications based on ArkCase and ADF, instantly scale up as your workload grows, and instantly scale down based on demand. Customers need to be confident that their existing infrastructure can handle a spike in traffic and that the spike will not interfere with normal business operations. Elastic Load Balancing and Auto Scaling can automatically scale a customer's AWS resources up to meet unexpected demand and then scale those resources down as demand decreases.

Measured Service

AWS uses automated monitoring systems to provide a high level of service performance and availability. Proactive monitoring is available through a variety of online tools both for internal and external use. Systems within AWS are extensively instrumented to monitor key operational metrics. Alarms are configured to notify operations and management personnel when early warning thresholds are crossed on key operational metrics. An on-call schedule is used such that personnel are always available to respond to operational issues. This includes a pager system so alarms are quickly and reliably communicated to operations personnel.

8.1.4 A successful Offeror will have the ability to provide cloud-based services through the following deployment methods:

Solutions built using the ADF can be deployed on any cloud-based model that includes

- Private Cloud
- Community Cloud
- Public Cloud
- Hybrid-Cloud
- On-Premise

The use of containerized deployment for reusable services using Kubernetes and Docker in ADF components allows the solutions developed using ADF to be easily deployed to any environment.

6.2 SubContractors

8.2.1 Offerors must explain whether they intend to provide all cloud solutions directly or through the use of Subcontractors.

Armedia is fully qualified to provide all cloud solutions directly without the use of Subcontractors. Our more than eight (8) years of past performance experience demonstrates Armedia's ability to provide these PaaS services without the use of Subcontractors.

8.2.2 Offeror must describe the extent to which it intends to use subcontractors to perform contract requirements.

Armedia does not intend to use subcontractors to perform contract requirements.

8.2.3 If the subcontractor is known, provide the qualifications of the subcontractor to provide the services; if not, describe how you will guarantee selection of a subcontractor that meets the experience requirements of the RFP.

This section is not applicable to Armedia's offer. We do not intend to use subcontractors to perform contract requirements.

6.3 Working with Purchasing Entities

8.3.1 Offeror must describe how it will work with Purchasing Entities before, during, and after a Data Breach, as defined in the Attachments and Exhibits

6.3.1 After a Data Breach

	Purchasing Entity Developed Solutions	Armedia Developed Solutions
Personnel involvement	If the Purchasing Entity uses the ADF to create custom solutions for its customers, the Purchasing Entity will be responsible for handling any data breaches on their custom solutions. Armedia support will be available based on the purchased service levels.	Armedia will be responsible for handling any data breach for solutions that Armedia develops on behalf of the Purchasing Entity using the ADF.
	Armedia's support staff will respond to any requests received from the Purchasing Entity pursuant to the terms of the purchased support levels.	Armedia's support staff will respond to any data breach on a priority basis as soon as it is detected or reported and will notify the concerned parties as per the SLAs.
Response Times	Response times will be determined by the Purchasing Entity. Armedia's response times to the Purchasing Entity will be based on the purchased support contract.	Armedia shall immediately notify (within 24 hours) Purchasing Entity if Armedia becomes aware of any accidental or unauthorized disclosure, access or use of any Personal Information or Confidential Information or a violation of applicable privacy or data protection laws (a "Breach") or if Armedia receives an access request, investigative notice, seizure or complaint from a government or data subject related to Purchasing Entity's Confidential Information (unless such
Remediation	The remediation process and timelines will be defined by the Purchasing Entity	

	Purchasing Entity Developed Solutions	Armedia Developed Solutions
		notification is prohibited). Armedia shall use its best efforts to immediately remedy any Breach and prevent any further Breach at its sole expense. In the event of any such Breach, Armedia shall immediately coordinate with Purchasing Entity regarding the response to, and investigation of, the Breach, and cooperate fully with Purchasing Entity, including facilitating interviews with employees and other parties, making available all relevant records, logs, files, data reporting and other materials, and providing Purchasing Entity with physical access to the facilities affected. In the event of a Breach of Personal Information in Armedia's possession or otherwise caused by or related to Armedia's acts or omissions, and without limiting Purchasing Entity's other rights and remedies, Armedia will pay all reasonable costs and expenses of any disclosures and notification required by applicable law or as otherwise determined as appropriate in Purchasing Entity's reasonable discretion, monitoring and reporting on the impacted individuals' or entities' credit records if determined in Purchasing Entity's reasonable discretion as reasonable to protect such individuals, and all other costs incurred by Purchasing Entity in responding to and mitigating damages caused by such Breach.
Communication	The methods of communication will be defined by the Purchasing Entity	Armedia will notify the Purchasing Entity and their affected Customers via emails of any data breach detected. The remediation and the

	Purchasing Entity Developed Solutions	Armedia Developed Solutions
		steps taken will also be communicated through emails. Armedia also recommends setting up change control boards comprising of Armedia PM, Purchasing Entity and its Customers' staff and having periodic CCB meetings where the breaches and the remediation can be communicated

Armedia will work with Purchasing Entity to modify the Figure 3 - Armedia Standard Language to Govern Data and Data Breaches. Armedia understands the trust that comes with managing a customer's data and we will use the best practices that we have employed with supporting our Top-Secret clients for over 16 years to include FBI, Joint Staff, and DIA.

5.3.1.1 Use. Confidential Information of the other party will be used solely as necessary to fulfill obligations under this Agreement and for no other purpose whatsoever. Confidential Information of the other may be disclosed internally on a "need to know" basis and shall not be made available to any third party except as specifically authorized by the disclosing party in writing. The receiving party agrees that nothing in this Agreement grants to the receiving party any license, right, title, or interest in or to the Confidential Information, except as expressly set forth herein. The parties agree to protect the other's Confidential Information using the same degree of care they use to protect their own confidential information of a like nature, but never less than ordinary care. Within thirty (30) days of the termination of this Agreement, or promptly upon the disclosing party's written request, the receiving party (i) will cease using and delete/destroy or return the disclosing party's Confidential Information and (ii) provide written confirmation to disclosing party upon request.

5.2 Exclusions/Exceptions. Confidential information does not include information that: (i) was known to a receiving party without restriction before receipt from the disclosing party; (ii) is publicly available through no fault of the receiving party; (iii) is rightfully received by the receiving party from a third party without a duty of confidentiality; or, (iv) is independently developed by the receiving party without reference to any Confidential Information. A receiving party may disclose Confidential Information as necessary to comply with a valid judicial or other governmental order, provided that the receiving party shall: (i) give the disclosing party reasonable written notice, to the extent permitted by law, and an opportunity to object prior to such disclosure; (ii) seek confidential treatment similar to the terms provided in this Agreement of such Confidential Information; and, (iii) comply with any applicable protective order or its equivalent.

5.3 Remedies. In the event of actual or threatened breach of the foregoing Confidential Information provisions resulting in immediate, substantial and irreparable harm to the disclosing party and the disclosing party will have no adequate remedy at law, the disclosing party may seek immediate injunctive and other equitable relief, without bond and without the necessity of showing actual money damages.

5.4 Data Security; Personal Information.

a. Personal Information. Offeror hereby acknowledges that during the performance of this Agreement, Offeror may have access to, collect, receive, transmit and/or store information that identifies or could identify (or potentially be matched with) Purchasing Entity's clients, consumers, employees, contractors or business partners, including but not limited to names, addresses, phone numbers, email addresses, job titles, dates of birth, user names, passwords, IP addresses, locations, Social Security or other identification numbers, health information, biometric data, financial account numbers or credit card information (all hereinafter,

"Personal Information"). To the extent that Offeror uses subcontractors that may have access to, collect, receive, transmit or store Personal Information, Offeror will notify Purchasing Entity of such subcontractors and ensure that such subcontractors execute written agreements agreeing to bound by and comply with the terms set forth in this Section.

b. Standard of Care. The Personal Information may only be used by Offeror for the purpose of providing Services under this Agreement and any other statements of work and in accordance with Purchasing Entity's instructions. Offeror will collect, store, transfer, dispose, disclose and use all Personal Information using the highest standard of care to ensure the integrity of such data and in compliance with all applicable federal, state and international privacy and data security laws, regulations and directives. In addition, Offeror shall: (i) use its best efforts to maintain administrative, technical, and physical safeguards that are no less vigorous than industry best practices to ensure the security and confidentiality of the Personal Information, protect against any anticipated threats or hazards to the security or integrity of the Personal Information, and protect against unauthorized access, use, or alteration of any Personal Information; (ii) not disclose any Personal Information to any person unless Purchasing Entity has given its prior written consent to such disclosure; and (iii) continually perform self-checks, including, but not limited to scanning for viruses and other contaminants to ensure that such software products have been found to be free of contaminants and viruses identifiable by such scans, and testing against publicized threats, data infiltrations and breaches to ensure the security and confidentiality of the Personal Information, in order to protect against unauthorized access, use, or alteration of the Personal Information. Upon termination of this Agreement for any reason, or upon request by Purchasing Entity, Offeror shall promptly return to Purchasing Entity all Personal Information, or at Purchasing Entity' request destroy all Personal Information and provide written certification to Purchasing Entity of such destruction.

c. Information Security. Offeror agrees that it will use its best efforts to implement administrative, technical, and physical safeguards that are no less vigorous that industry best practices to insure the security and confidentiality of Personal information and Confidential Information, protect against any anticipated threats or hazards to the confidentiality, availability or integrity of Personal Information and Confidential Information, and protect against unauthorized access, use or alteration of Personal Information and Confidential Information and will implement and thereafter maintain safeguards in accordance with agreed upon standard such as (i) the International Organization for Standardization's ISO/IEC 27001:2013 and ISO/IEC 27002:2013 standards or (ii) Health Information Trust Alliance (HITRUST) Certification or (iii) FedRAMP or (iv) DoD Impact Levels, to ensure the security and confidentiality of Personal Information and Confidential Information, protect against any anticipated threats or hazards to the confidentiality, availability or integrity of Personal Information and Confidential Information, and protect against unauthorized access, use, or alteration of Personal Information and Confidential Information. Upon Purchasing Entity's request, Offeror shall promptly and accurately complete a written information security assessment questionnaire provided by Purchasing Entity regarding Offeror's information technology environment; Offeror will at all times during the Term maintain information security protections no less secure than the practices identified by Offeror in such questionnaire. At a minimum, Offeror shall maintain a comprehensive written information security program managed by one or more designated employees with safeguards that include limiting access to Personal Information and Confidential Information to only employees and authorized Subcontractors who need access to carry out Services under this Agreement, securing business facilities, data centers, paper files, services, back-up systems, computing equipment and mobile devices where Personal Information and Confidential Information is stored, implementing network, device, database and platform security, securing information transmission, storage and disposal, implementing authentication and access controls within media, applications, operating systems and equipment, encrypting sensitive Personal Information

(including social security numbers, financial account numbers and health information) during mobile storage and transmission, strictly segregating Personal Information from information of Offeror or its other clients, implementing appropriate personnel security and integrity procedures and practices, providing appropriate privacy and information security training to Offeror's employees and Subcontractors, continually performing self-checks, including, but not limited to scanning for viruses and other contaminants to ensure that such software products have been found to be free of contaminants and viruses identifiable by such scans, and testing against publicized threats, data infiltrations and breaches to ensure the security and confidentiality of Personal Information, and establishing and enforcing written policies regarding the collection, storage, transfer, disclosure, use and disposal of Personal Information and a disciplinary process for employees violating such policies. Offeror shall continually identify and assess reasonably foreseeable internal and external threats and vulnerabilities and, at its sole cost and expense, promptly correct all identified security deficiencies or vulnerabilities that may compromise the security of Personal Information or Confidential Information. Offeror shall also adhere to any of Purchasing Entity's policies, standards, procedures and guidelines provided by Purchasing Entity with respect to the collection, classification and handling of Personal Information and Confidential Information.

d. Data Breaches. Offeror shall immediately notify (within 24 hours) Purchasing Entity if Offeror becomes aware of any accidental or unauthorized disclosure, access or use of any Personal Information or Confidential Information or a violation of applicable privacy or data protection laws (a "Breach") or if Offeror receives an access request, investigative notice, seizure or complaint from a government or data subject related to Purchasing Entity's Confidential Information (unless such notification is prohibited). Offeror shall use its best efforts to immediately remedy any Breach and prevent any further Breach at its sole expense. In the event of any such Breach Offeror shall immediately coordinate with Purchasing Entity regarding the response to, and investigation of, the Breach, and cooperate fully with Purchasing Entity, including facilitating interviews with employees and other parties, making available all relevant records, logs, files, data reporting and other materials, and providing Purchasing Entity with physical access to the facilities affected. In the event of a Breach of Personal Information in Offeror's possession or otherwise caused by or related to Offeror's acts or omissions, and without limiting Purchasing Entity's other rights and remedies, Offeror will pay all reasonable costs and expenses of any disclosures and notification required by applicable law or as otherwise determined as appropriate in Purchasing Entity's reasonable discretion, monitoring and reporting on the impacted individuals' or entities' credit records if determined in Purchasing Entity's reasonable discretion as reasonable to protect such individuals, and all other costs incurred by Purchasing Entity in responding to and mitigating damages caused by such Breach.

e. Cross-Border Transfers. When and as required by Purchasing Entity from time to time, Offeror shall promptly execute and/or shall cause its Affiliate(s) or subcontractor(s) to execute supplemental privacy and security terms, including but not limited to the Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries, dated 5 February 2010 (2010/87/EU), as amended from time to time ("EU Model Contract"), with Offeror or Affiliated companies that provide services under the Agreement as required in Purchasing Entity's sole judgment for the processing and/or transfer of Personal Information in accordance with applicable law. If Offeror will be knowingly transferring Personal Information from, to, or through the European Union, Offeror shall at all relevant times for purposes of this Agreement maintain a current certification status with the US-EU Safe Harbor Privacy Arrangement to protect Personal Information, unless Offeror has notified Purchasing Entity that it does not maintain such a certification and executes an EU Model Contract with Purchasing Entity. Offeror will provide Purchasing Entity with ninety (90) days written notice prior to any date on which Offeror's current Safe Harbor certification status ends.

Audits. Offeror shall comply with all requests from Purchasing Entity to certify Offeror's ongoing compliance with the provisions of this section. Offeror shall provide Purchasing Entity with copies of any applicable Payment Card Industry Data Security Standards (PCI DSS), Statement on Standards for Attestation Engagements No. 16 (SSAE 16), Service Organizations Controls (SOC1, 2 or 3) or Health Insurance Portability and Accountability Act (HIPAA) audits current as of the execution of this Agreement or conducted during the Term. Purchasing Entity reserves the right for it or a third party to conduct a full security audit, assessment or review, including, but not limited to, penetration or vulnerability testing of Offeror's network and systems and physical and technical environment, to identify the strengths and weaknesses of existing security arrangements. Offeror shall fully cooperate with such audit by providing access to knowledgeable personnel, physical premises, documentation and infrastructure unless Offeror security officer reasonably deems such access a threat to Offeror confidentiality and security.

Figure 3 - Armedia Standard Language to Govern Data and Data Breaches

6.3.2 Prohibition of Adware Etc.

8.3.2 Offeror must describe how it will not engage in or permit its agents to push adware, software, or marketing not explicitly authorized by the Participating Entity or the Master Agreement.

The ACC and ADF have no adware software and provide no integration with any such tools. Use of any adware in ACC is forbidden.

6.3.3 Testing/Staging Environment

8.3.3 Offeror must describe whether its application-hosting environments support a user test/staging environment that is identical to production.

Armedia develops and maintains the ADF and ACC offerings. Development and testing of ADF is done within Armedia's on-premise installations before the new release is pushed to an AWS cloud staging environment. Based on the PaaS agreement, the Purchasing Entity can use Armedia to create a test and staging environment for the Purchasing Entity to test and validate the custom applications built by the Purchasing Entity using ADF. Armedia recommends setting up at least 3 environments at a minimum – Testing and Integration, Pre-production and Production with Pre-Production and Production environments being mirror copies of each other while the Testing and Integration environment being a scaled down version of Production for cost benefits.

6.3.4 508 Compliance

8.3.4 Offeror must describe whether or not its computer applications and Web sites are accessible to people with disabilities and must comply with Participating Entity accessibility policies and the Americans with Disability Act, as applicable.

ADF ships with an Angular based, responsive web application that can be customized and extended based on the specific requirements of the customer. The web application included with ADF has built-in 508-compliance and internationalization features. See Appendix A: ArkCase VPAT and Appendix B: Alfresco VPAT.

The Purchasing Entity however, is free to use any alternate web application interface that supports REST API-based application development. The Purchasing Entity will be responsible for maintaining 508-compliance for the custom web application developed by the entity.

6.3.5 Browser Platforms

8.3.5 Offeror must describe whether or not its applications and content delivered through Web browsers are be accessible using current released versions of multiple browser platforms (such as Internet Explorer, Firefox, Chrome, and Safari) at a minimum.

ADF ships with an Angular based, responsive web application that can be customized and extended based on the specific requirements of the customer. The web application included with ADF works with the latest versions of all known browsers including Internet Explorer, Firefox, Chrome and Safari. The Purchasing Entity is responsible for maintaining browser compatibility and 508-compliance when creating custom applications using ADF.

6.3.6 Personal Information

8.3.6 Offeror must describe how it will, prior to the execution of a Service Level Agreement, meet with the Purchasing Entity and cooperate and hold a meeting to determine whether any sensitive or personal information will be stored or used by the Offeror that is subject to any law, rule or regulation providing for specific compliance obligations.

Armedia will facilitate a meeting with Purchasing Entity and cooperate and hold a meeting to determine whether any sensitive or personal information will be stored or used by the Purchasing Entity. In addition, we will document any law, rule or regulation for which we need to comply as well as define information access, retention, and destruction requirements. Figure 3 - Armedia Standard Language to Govern Data and Data Breaches, contains a section that defines PII and will be reviewed and updated pursuant to the meeting with Purchasing Entity.

6.3.7 Project Schedule Plans

8.3.7 Offeror must describe any project schedule plans or work plans that Offerors use in implementing their Solutions with customers. Offerors should include timelines for developing, testing, and implementing Solutions for customers.

Based on our past experiences with our customers like USDA, PAHO etc., Armedia recommends using the proven project development and delivery approached outlined below (Figure 4) when developing custom applications using ADF and ACC.

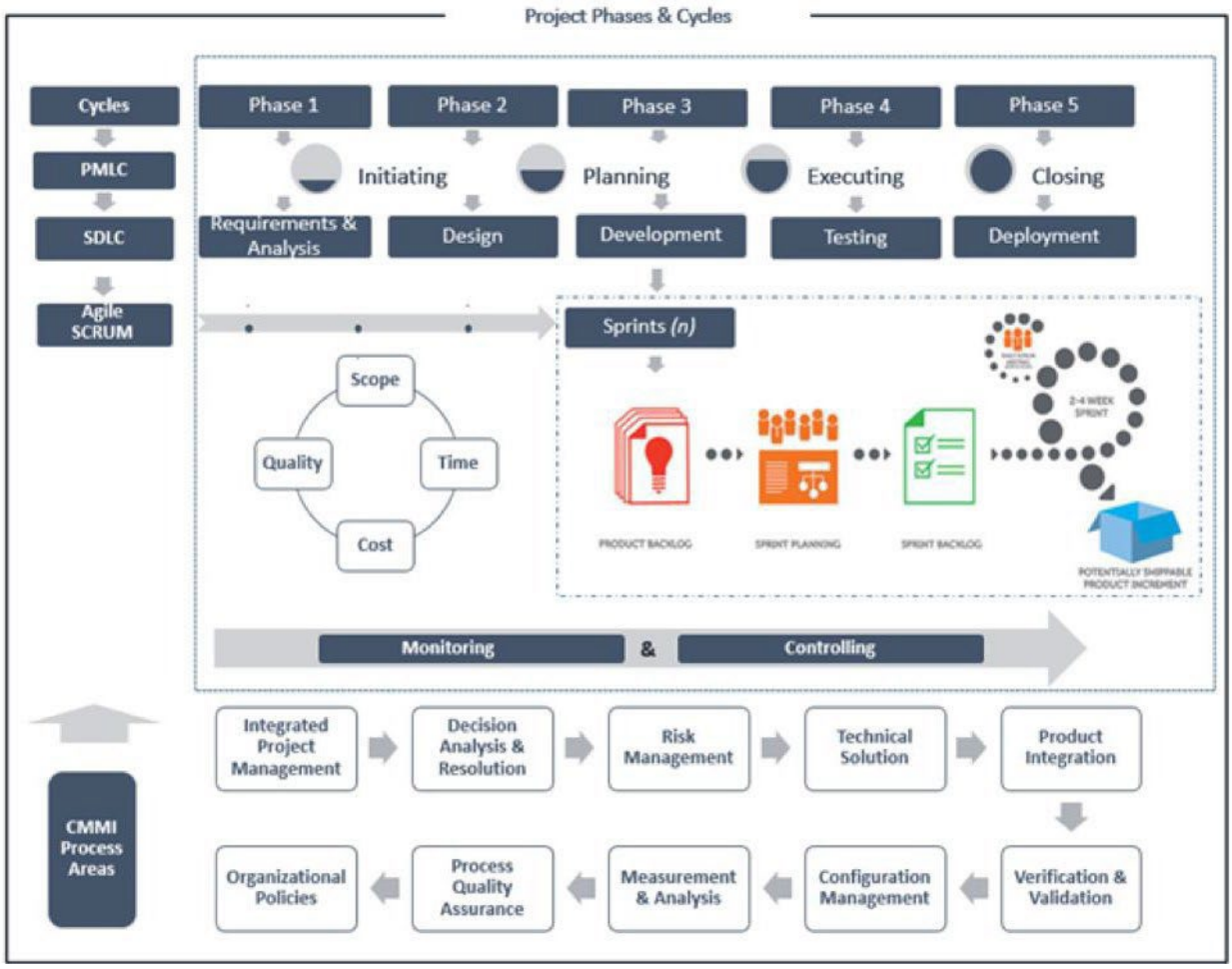


Figure 4 - Armedia's recommended Project Management Plan when developing custom solutions using ADF and ACC

6.3.7.1 Delivery Stages

When Armedia is contracted to develop and deliver custom solutions on behalf of the Purchasing entity, we will fulfill our committed project activities, tasks and deliverables within five **Project Delivery Phases**. The stages and accompanying processes may be *tailored* based on our client's business needs, requirements, operating procedures, or technical environment. A decision whether to adjust Armedia's standard phases and process for any individual client is determined during the Project Kickoff. Following the kickoff, the project moves into the Planning Phase. At that time, the Project Manager creates the defined project processes by tailoring the Armedia standard delivery processes to the client-requested cost, schedule, business, and technical requirements. These tailored processes are documented in the Project Management Plan. The PMP creates a context for the project. It represents agreement with the client on the defined processes.

6.3.7.1.1 Phase 1 – Initiation and Requirements and Analysis

The first delivery Phase consists of the following, initial, high-level project activities.

6.3.7.1.1.1 Project Kickoff

The official start of the project initiates communication and collaboration between the Armedia project team and the system stakeholders. The Project Kickoff meeting solidifies a common understanding of the work, tasks, methodology, and deliverables.

6.3.7.1.1.2 Discovery Workshops

The lead Business Analyst (BA) will schedule workshops (i.e., Joint Application Development – JAD -- sessions) with system stakeholders to review and collect functional and non-functional requirements. The business requirements included in the statement of work will be reviewed, decomposed, and validated with the stakeholders to ensure corporate understanding. In addition, the Armedia team will work closely with the current developers and the stakeholders to ensure a thorough and expedient transition of knowledge occurs.

Following validation of the requirements, the BA will create a Requirements Traceability Matrix (RTM) and (with the project's Technical Lead), perform a gap analysis or reasonability assessment to map the requirements to the system solution. This mapping will identify gaps in the design and/or technology by comparing the known capabilities of the solution and technology with the needs of the stakeholders, as expressed in the requirements. These gaps will then be presented to the stakeholders for further requirements development or mitigation.

6.3.7.1.2 Phase 2 – Planning and Design

The Project Manager plans and schedules the technical activities, producing the Work Breakdown Structure (WBS) and the detailed Project Schedule. The PM creates the defined project processes by tailoring the Armedia standard delivery processes to the system requested cost, schedule, and technical requirements.

6.3.7.1.2.1 Requirements review and preliminary design

The BA and Technical Lead review the RTM. The BA will update any content- or technical-related constraints. When the RTM is agreed to, the Technical Lead creates the conceptual design to include any data and security constraints or concerns, the ITLC security checklist, and the deliverable expectation documentation (DED). The system stakeholders will review and approve the RTM, the conceptual design, and the ITLC checklist, and the DED. Though this is a serial, or waterfall, sequence of events, the entire process may be repeated for each new module or package of system enhancements.

6.3.7.1.2.2 Design

The system requirements are core to the design and engineering of the technical solution. The Technical Lead is responsible for ensuring that the technical solution correctly fits both the system business needs and the operating environment. Team Armedia will update the Design Specification document which may include the system architecture, security, data structures, protocols, components, and interfaces. The system stakeholders will review and approve the Design Specification document before development begins. Though this is a serial, or waterfall, sequence of events, the entire process may be repeated for each new module or package of system enhancements.

6.3.7.1.3 Phase 3 – Development and Execution

The project team will develop, test, and deliver the solution within an Agile sprint-based framework. The Agile approach quickly delivers functionality and actively involves the system stakeholders and users.

6.3.7.1.3.1 Project Management

The PM oversees all project activities, issues, change requests, and risks. The Risk Management Plan is devoted to this critical provision. The PM proactively identifies and mitigates risk from project initiation to closure.

6.3.7.1.3.2 System Engineering

The Armedia System Engineer establishes configuration management processes like source code control, continuous integration, static and dynamic code analysis, automated build and deployments, monitoring, and tuning. Where feasible, these processes will leverage the FDACS Microsoft Team Foundation Server (TFS).

6.3.7.1.3.3 Development

Fully conversant with the system requirements design, the Development Team codes the integrated system components. The team follows the FDACS published Internet web standards for configuration, continuous development, unit testing, and code reviews.

6.3.7.1.3.4 Test

To validate 100 percent requirements coverage, the Testers develop test cases/scripts that map to the system Requirements Traceability Matrix (RTM).

6.3.7.1.4 Phase 4 – Testing

As an overarching *Phase*, monitoring and control is a continuous activity integrated into the entire project life cycle.

6.3.7.1.4.1 Regular Measurement

The Project Manager regularly monitors and takes measurements of the delivery progress. The sooner that the PM can identify variances from the project plan, the less impact they will have. The PM can quickly take corrective action to realign the plan to the project objectives.

6.3.7.1.4.2 Product Control

Testing is our frontline control of product quality. The system solution, as a single functional component, will be tested, verified, and validated against the system requirements. The Test Plan describes the types of tests required (i.e., system integration, performance and user acceptance) and the use of testing tools. Where feasible, all test cases, test data, and test results will be managed in TFS.

6.3.7.1.4.3 Documentation

User documentation will be updated or created to address enhancements to the existing system, and new modules as they are delivered.

6.3.7.1.4.4 User Acceptance Testing

In accordance with the Project Test Plan and the test cases, the Test Team coordinates, supports and executes the System Acceptance and User Acceptance tests. Preparation covers requirements for both internal system testing and external client acceptance testing. The Armedia team follows standard procedure for reporting, correcting, and retesting defects.

6.3.7.1.4.5 Project Financials and Schedule Reporting

Two integrated project plans are appended to the Project Management Plan: Cost Management Plan and Schedule Management Plan. The plans describe the respective monitoring and control guidelines. The Project Manager tracks actual costs and schedule against planned costs and schedule for each Sprint. The PM establishes the metrics and, with the system Project Manager, refines them. Reporting is made monthly.

6.3.7.1.5 Phase 5 – Deployment and Closing

The final Phase formally concludes the system project phase and addresses the activities for turning over the completed solution to the Operations and Maintenance (O&M) team for ongoing support.

6.3.7.1.5.1 System Acceptance

The System Acceptance and Go/No Go criteria is determined during Operations Readiness Review (ORR) meeting with our client's stakeholders, and the Armedia project and Operations and Maintenance (O&M) teams. The purpose of the Operations Readiness Review is to ensure that the project has followed a defined software development process, and that the project team has identified system interdependencies and risks that may have an adverse impact on the organization, and/or the software application/system deployment. The Readiness Review also confirms that appropriate departments have been notified and are fully aware of all pending releases and the potential impact. In this document, risk mitigation strategies and contingency plans are also defined, to help eliminate any adverse impact that may result from the release.

6.3.7.1.5.2 Deployment

In collaboration with the system Project Manager and stakeholders, the Project Manager ensures that 1) system users are properly trained and aware, 2) system technical resources are properly trained and available, and 3) Armedia is fully staffed to provide technical support.

6.3.7.1.5.3 Incident Monitoring

After deploying each component of the system solution, the team will closely monitor incident reports and the Armedia defect tracking database to analyze trends and identify potential enhancements. The PM (or designated team member) will record any resulting enhancements and submit for approval to system, per the established change control process. When approved, these enhancements will be added to the Requirements Traceability Matrix and appropriately scheduled for a release cycle.

6.3.7.1.5.4 Evaluation

In the spirit of project collaboration, Armedia will solicit system user feedback and add it to the solution evaluation report. Our O&M Project Manager and the project team will capture and evaluate lessons learned. Reinforcing our commitment to continuous improvement, we will incorporate into our management processes relevant and constructive findings in the lessons learned and the stakeholder feedback.

6.3.7.1.5.5 Closing

The closing stage of the project includes ensuring all deliverables have been turned over, all contracted obligations have been met, and any lessons learned during the project have been documented for future reference. Knowledge transfer activities should be completed. Any remaining payments or remaining funds should be processed.

6.3.7.2 Delivery Approach

Armedia proposes a hybrid Waterfall-Agile approach, using a Waterfall methodology for the requirements, planning, and high-level design phases, and an Agile methodology for the component design and development phase. We see this approach as beneficial in developing solutions for several reasons. By engaging the stakeholders upfront and early in the process to gather requirements under a Waterfall methodology, Armedia is able to develop a roadmap that

will fully identify and validate the critical business requirements for our client. This will not only produce meaningful milestones but will also set the right expectations.

For development of the custom solutions using ADF and ACC, Armedia proposes an Agile methodology. We will begin with a typical, four-week cycle for each Sprint, but will coordinate with the customer and adjust Sprint durations as necessary to meet the demands of the project. Each Sprint will provide business owners and users with a one-week validation of the functionality of the Sprint. This method will benefit our client by providing continuous feedback and allow the Armedia development team to promptly address feedback.

6.3.8 Service Updates

8.3.8 The State of Utah expects Offeror to update the services periodically as technology changes. Offer must describe:

- *How Offeror's services during Service Line Additions and Updates pursuant to section 2.12 will continue to meet the requirements outlined therein.*

Armedia is committed to providing great service to its customers through continuous improvements and innovations on ADF and ACC. Armedia development teams work directly with customers to ensure that innovation on the ACC and ADF is driven by customer demand, and we continuously evolve and improve our existing services and frequently add new services. Armedia's typical release cycle is 3-6 months for minor releases and 18-24 months for major releases. Patch releases to address an immediate concern are also scheduled. To attract and retain Purchasing Entities, Armedia understands that Purchasing Entities have options and we must provide compelling offerings that are secure, intuitive, modern and flexible to support a fluid environment.

- *How Offeror will maintain discounts at the levels set forth in the contract.*

As with Armedia's GSA Schedules that Armedia has maintained for over ten years, Armedia will maintain discounts as the levels set forth in the contract.

- *How Offeror will report to the Purchasing Entities, as needed, regarding changes in technology and make recommendations for service updates.*

Armedia provides periodic updates to the ADF components. These updates along with the release notes will be made available to the Purchasing Entities and their customers. The Purchasing Entity will be responsible of applying these updates to their applications developed using ADF for their customers at their discretion.

- *How Offeror will provide transition support to any Purchasing Entity whose operations may be negatively impacted by the service change.*

Any updates made to the ACC – that includes applying security patch releases to the ACC offerings that may impact the Purchasing Entity – will be communicated with the Purchasing Entity along with the expected service outage time if any.

6.4 Customer Service

ENSURING EXCELLENT CUSTOMER SERVICE

8.4.1 Offeror must describe how it will ensure excellent customer service is provided to Purchasing Entities. Include:

- *Quality assurance measures;*
- *Escalation plan for addressing problems and/or complaints; and*
- *Service Level Agreement (SLA).*

COMPLIANCE WITH CUSTOMER SERVICE REQUIREMENTS

8.4.2 Offeror must describe its ability to comply with the following customer service requirements:
a. You must have one lead representative for each entity that executes a Participating Addendum. Contact information shall be kept current.
b. Customer Service Representative(s) must be available by phone or email at a minimum, from 7AM to 6PM on Monday through Sunday for the applicable time zones.
c. Customer Service Representative will respond to inquiries within one business day.
d. You must provide design services for the applicable categories.
e. You must provide Installation Services for the applicable categories.

Armedia's technical support for ACC PaaS is a one-on-one, fast-response support channel that is staffed 24x7x365 with AWS certified and experienced technical support engineers. The service helps customers of all sizes and technical abilities to successfully use ACC for their custom applications developed using ADF and ArkCase.

Armedia also provides detailed release notes with every release of the ADF along with the code quality coverage reports and test results as part of Armedia Qaulity Assurance for the ADF PaaS offering.

Armedia Support Features for ACC PaaS

Armedia Support provides a highly personalized level of service for customers seeking technical help. Customers who do not choose Armedia Support will continue to have access to Basic Support offered at no additional charge. Besides the Basic Support – included with the ACC PaaS offering – Armedia offers a flat rate support plan (Enterprise Support) for ACC that is available to the Purchasing Entities on a monthly subscription basis. All plans, including Basic Support, provide 24x7 access to customer service, ACC Documentation, Resource Center, Product Wiki and FAQs, Discussion Forums, and support for Health Checks.

Contacting Armedia Support

Customers can contact Armedia Support via the Support Center. All Developer-level support customers can open a case online using a web browser. Customers with a paid enterprise support subscription will be able to call Armedia Support or strike up a conversation with an engineer via Chat.

Chat is another way to contact Armedia Support. By clicking on the chat support icon in the Support Center, a chat session will be initiated through the browser. This provides a real-time, one-on-one interaction with our support engineers and allows additional information and links to be shared for faster issue resolution.

	Basic	Enterprise
Customer Service – 24x7x365	✓	✓
Support Forums	✓	✓
Documentation, Whitepapers, Best Practice Guides	✓	✓

	Basic	Enterprise
Access to Technical Support	Support for Health Checks	Phone, Chat, Email, Technical Account Manager (TAM) (24/7)
Primary Case Handling	Technical Customer Service Associate	ACC PaaS support engineer
Users Who Can Create Technical Support Cases		5
Response Time		General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour Business-critical system down: < 15 minutes
Architecture Support		Contextual Application Architecture Guidance
Access to Support API		✓
Third-Party Software Support		✓
Infrastructure Event Management		Contact us for pricing
Architectural Review		✓
Support Concierge		✓
Operations Support		Operational reviews, recommendations, and reporting

6.5 Security of Information

6.5.1 Protection of Data

8.5.1 Offeror must describe the measures it takes to protect data. Include a description of the method by which you will hold, protect, and dispose of data following completion of any contract services.

Data in Armedia's PaaS and SaaS offerings is protected through a number of means including, but not limited to data encryption (including encryption of data both in transit and at rest), access control, system integrity protection (to protect against and protect from threats such as malware), and network-level defenses (to protect against and protect from network-based attacks). Following the completion of any contract services, Armedia will hold, protect, transfer or dispose of applicable customer data as appropriate. This will be achieved through the following process:

- Identification of customer data requirements beyond those already identified
- Archiving of any data required by the customer for duration specified by the Purchasing Entity and their customers using Amazon Glacier
- Secure transfer of archived data to the customer as required using Amazon's bulk data transfer tool – AWS Import/Export Disk and AWS Snowball Edge – a data transport solution that uses devices designed to be secure to transfer large amounts of data into and out of the AWS Cloud.
- Deletion of customer data from Armedia PaaS and/or SaaS systems using the AWS techniques compliant with the process detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.
- Deletion of customer data from Armedia-controlled backup that is built on AWS Glacier and DR systems when the Purchasing Entity uses a DR setup for the ADF based custom applications.

6.5.2 Compliance with Data Privacy/Security Regulations

8.5.2 Offeror must describe how it intends to comply with all applicable laws and related to data privacy and security.

Armedia uses FedRAMP security controls as the baseline for its security testing for all the services offered in the ADF and ACC. The Purchasing Entities are open to design additional security controls that comply with all applicable laws and regulations related to data privacy and security for its customers as needed. In the event of Armedia being contracted to develop custom solutions for the Purchasing Entity using ADF, Armedia will work with the Purchasing Entity to comply with any additional security controls not already covered by the FedRAMP controls. The process utilized for this consists of the following:

- Identification of applicable laws and regulations with customers during project specification
- Identification of any gaps in PaaS and/or SaaS processes due to laws and regulations identified in the previous step
- Modification of processes as required in order to achieve full compliance with applicable laws and regulations related to data privacy and security

6.5.3 Purchasing Entity's User Accounts

8.5.3 Offeror must describe how it will not access a Purchasing Entity's user accounts or data, except in the course of data center operations, response to service or technical issues, as required by the express terms of the Master Agreement, the applicable Participating Addendum, and/or the applicable Service Level Agreement.

Armedia personnel will not access any Purchasing Entity's user accounts or data, except in the course of data center operations, response to service or technical issues, as required by the express terms of the Master Agreement, the applicable Participating Addendum, and/or the applicable Service Level Agreement. Armedia systems are designed with a *least privilege* philosophy, which limits Armedia personnel access to customer data through technical control methods such as access control. Additionally, Armedia personnel are barred by Armedia policy from accessing customer

data for any unauthorized purposes. Also, all customer data on ACC is stored on encrypted storage devices providing additional data security at rest.

6.6 Privacy and Security

6.6.1 NIST Compliance

*8.6.1 Offeror must describe its commitment for its Solutions to comply with NIST, as defined in NIST Special Publication 800-145, and any other relevant industry standards, as it relates to the Scope of Services described in **Attachment D**, including supporting the different types of data that you may receive.*

Armedia's PaaS and SaaS offerings are designed and operated as cloud-based services, as defined in NIST Special Publication 800-145 (see responses to Requirements of Attachments C & D). In addition, Armedia follows applicable information security controls for a Moderate impact system from NIST Special Publication 800-53 as a configuration, architectural, and operational baseline.

6.6.2 Security Certifications

8.6.2 Offeror must list all government or standards organization security certifications it currently holds that apply specifically to the Offeror's proposal, as well as those in process at time of response.
Specifically include HIPAA, FERPA, CJIS Security Policy, PCI Data Security Standards (DSS), IRS Publication 1075, FISMA, NIST 800-53, NIST SP 800-171, and FIPS 200 if they apply.

A CSA STAR self-assessment has been completed for Armedia's PaaS and SaaS offerings, and the results of that self-assessment are attached to this response.

ACC is built using NIST 800-53 compliant AWS resources and infrastructure that has been designed and is managed in alignment with regulations, standards, and best practices, including:

- Federal Risk and Authorization Management Program (FedRAMP)
- National Institute of Standards and Technology (NIST) 800-171
- Federal Information Security Management Act (FISMA)
- Federal Information Processing Standard (FIPS) 140-2
- Department of Defense (DoD) Security Requirements Guide (SRG) Impact Levels 2, 4, 5, and 6
- FBI Criminal Justice Information Services (CJIS)
- US Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)
- International Organization for Standardization (ISO) 27001, 27017, 27018, and 9001
- International Traffic in Arms Regulations (ITAR)
- Family Educational Rights and Privacy Act (FERPA)
- System and Organization Controls (SOC) 1, SOC 2, and SOC 3

6.6.3 Security Practices

8.6.3 Offeror must describe its security practices in place to secure data and applications, including threats from outside the service center as well as other customers co-located within the same service center.

Armedia follows industry standard best practices in the area of information security and manages environments with a range of specific security requirements including compliance with:

- FedRAMP Moderate
- HITRUST
- HIPAA
- CJIS

Physical security for Armedia's PaaS and SaaS offerings is managed by Amazon, as all environments are hosted within AWS.

Protection of data from other ACC customers is accomplished through the use of AWS VPCs and AWS security groups. AWS security monitoring tools help identify several types of denial of service (DoS) attacks, including distributed, flooding, and software/logic attacks. When DoS attacks are identified, the AWS incident response process is initiated. In addition to the DoS prevention tools, redundant telecommunication providers at each region as well as additional capacity protect against the possibility of DoS attacks.

The ACC's use of AWS network provides significant protection against traditional network security issues, and you can implement further protection. The following are a few examples:

- **Distributed Denial of Service (DDoS) Attacks.** AWS API endpoints are hosted on large, Internet-scale, world-class infrastructure that benefits from the same engineering expertise that has built Amazon into the world's largest online retailer. Proprietary DDoS mitigation techniques are used. Additionally, AWS's networks are multi-homed across a number of providers to achieve Internet access diversity.
- **Man in the Middle (MITM) Attacks.** All of the AWS APIs are available via SSL-protected endpoints which provide server authentication. Amazon EC2 AMIs automatically generate new SSH host certificates on first boot and log them to the instance's console. You can then use the secure APIs to call the console and access the host certificates before logging into the instance for the first time. We encourage you to use SSL for all of your interactions with AWS.
- **IP Spoofing.** Amazon EC2 instances cannot send spoofed network traffic. The AWS-controlled, host-based firewall infrastructure will not permit an instance to send traffic with a source IP or MAC address other than its own.
- **Port Scanning**. Unauthorized port scans by Amazon EC2 customers are a violation of the AWS Acceptable Use Policy. Violations of the AWS Acceptable Use Policy are taken seriously, and every reported violation is investigated. Customers can report suspected abuse via the contacts available on our website at: http://aws.amazon.com/contact-us/report-abuse/. When unauthorized port scanning is detected by AWS, it is stopped and blocked. Port scans of Amazon EC2 instances are generally ineffective because, by default, all inbound ports on Amazon EC2 instances are closed and are only opened by you. Your strict management of security groups can further mitigate the threat of port scans. If you configure the security group to allow traffic from any source to a specific port, then that specific port will be vulnerable to a port scan. In these cases, you must use appropriate security measures to protect listening services that may be essential to their application from being discovered by an unauthorized port scan. For example, a web server must clearly have port 80 (HTTP) open to the world, and the administrator of this server is responsible for the security of the HTTP server software, such as Apache. You may request permission to conduct vulnerability scans as required to meet your specific compliance requirements. These scans must be limited to your own instances and must not violate the AWS Acceptable Use Policy. Advanced approval for these types of scans can be initiated

by submitting a request via the website at: https://aws-portal.amazon.com/gp/aws/html-forms-controller/contactus/AWSSecurityPenTestRequest

- **Packet sniffing by other tenants.** It is not possible for a virtual instance running in promiscuous mode to receive or "sniff" traffic that is intended for a different virtual instance. While you can place your interfaces into promiscuous mode, the hypervisor will not deliver any traffic to them that is not addressed to them. Even two virtual instances that are owned by the same customer located on the same physical host cannot listen to each other's traffic. Attacks such as ARP cache poisoning do not work within Amazon EC2 and Amazon VPC. While Amazon EC2 does provide ample protection against one customer inadvertently or maliciously attempting to view another's data, as a standard practice you should encrypt sensitive traffic.

6.6.4 Data Confidentiality

8.6.4 Offeror must describe its data confidentiality standards and practices that are in place to ensure data confidentiality. This must include not only prevention of exposure to unauthorized personnel, but also managing and reviewing access that administrators have to stored data. Include information on your hardware policies (laptops, mobile etc).

Armedia does not access the Purchasing Entity or their customer's data, and the Purchasing Entity is given the choice as to how they store, manage and protect their data.

Armedia ensures data confidentiality in its PaaS and SaaS offerings through means including the use of technical and policy access control measures. Armedia systems are architected using a *least privilege* philosophy. Access privileges granted to Armedia administrators are reviewed on at least an annual basis. Data in Armedia environments is securely encrypted, both in transit and at rest.

Armedia issues laptops to its employees and said laptops are used for tasks such as management of Armedia environments. Armedia environments are not managed through the use of personally owned mobile devices.

6.6.5 Third Party Security Credentials

8.6.5 Offeror must provide a detailed list of the third-party attestations, reports, security credentials (e.g., FedRAMP High, FedRAMP Moderate, etc.), and certifications relating to data security, integrity, and other controls.

Armedia currently has In Process designation from the FedRAMP PMO for a FedRAMP Moderate Impact offering. A third-party assessment organization has completed assessment of Armedia's FedRAMP offering, and Armedia anticipates a full FedRAMP authorization for said offering by September 2018.

6.6.6 Logging Process

8.6.6 Offeror must describe its logging process including the types of services and devices logged; the event types logged; and the information fields. You should include detailed response on how you plan to maintain security certifications.

The ADF components provides application level logging for all the services of the ADF which can be configured using a logging configuration dashboard accessible only to authorized personnel (Figure 5). These service logs record all interactions with the services through the REST API end-points at every event in standard java logging format which can be configured to be consumed and

analyzed by any log analysis tool that the Purchasing Entity desires to use. ADF ships with a configurable ElasticSearch instance that can be used for log analysis as well.

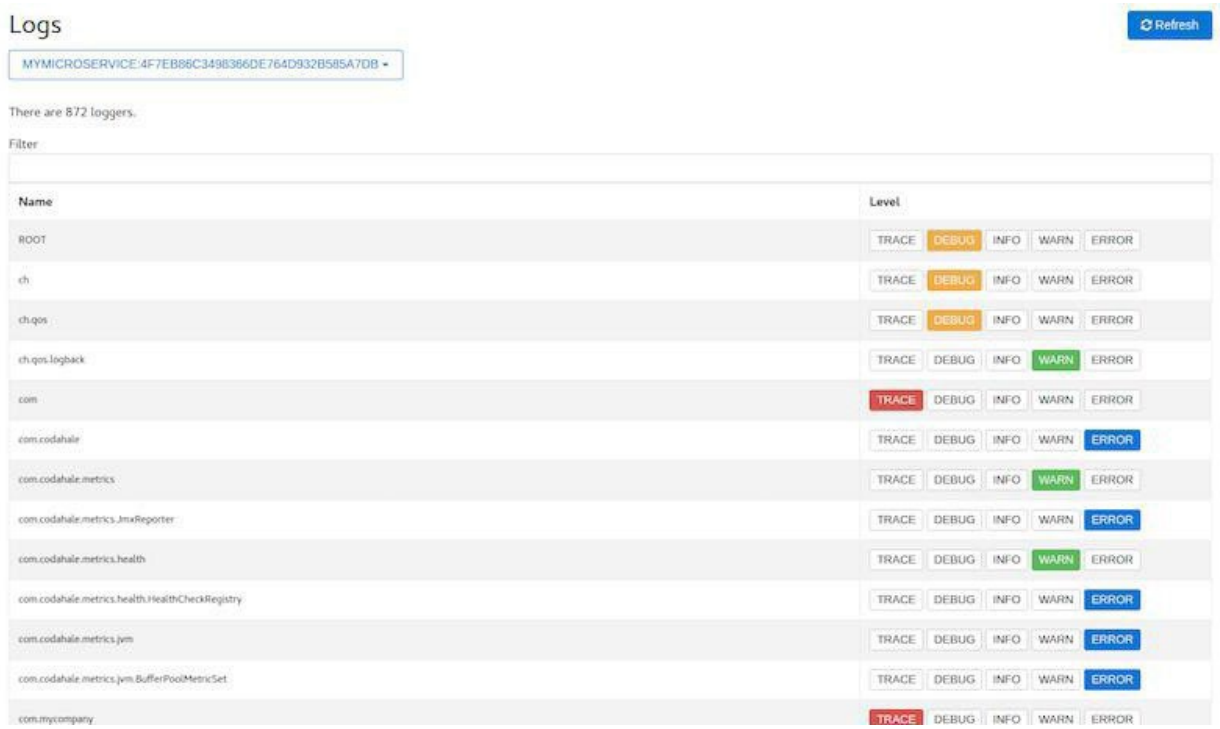


Figure 5 - Configuring logging for ADF based applications

6.6.7 Visibility of Data

8.6.7 Offeror must describe whether it can restrict visibility of cloud hosted data and documents to specific users or groups.

Armedia's PaaS and SaaS offerings provide the ability to restrict visibility of data and documents to specific users and groups. This is achieved through the use of role-based access control in said offerings. Customer environments are segregated from one another utilizing dedicated customer VPCs and AWS Security Groups. Additionally, multifactor authentication can be provided for customer environments in order to provide an additional level of data protection.

6.6.8 Notification Process

8.6.8 Offeror must describe its notification process in the event of a security incident, including relating to timing, incident levels. Offeror should take into consideration that Purchasing Entities may have different notification requirements based on applicable laws and the categorization type of the data being processed or stored.

The customer notification process utilized by Armedia for its PaaS and SaaS offerings in the event of a security incident are as follows:

- Initial triage of the event
- Notification of information security personnel if event not initially detected by information security personnel
- Notification of impacted parties (by email and/or phone depending upon specific requirements)

- Investigation and remediation (with additional notification as appropriate during these phases)
- Notification of final impact and lessons learned.

Specific timelines for each of these steps are dependent upon individual customer requirements and Service Level Agreements.

Additionally, ACC uses AWS notification mechanisms that are in place to allow the customer support team to be notified of operational issues that impact the customer experience. A "Service Health Dashboard" is available and maintained by the customer support team to alert customers to any issues that may be of broad impact.

6.6.9 Security on Hosted Servers

8.6.9 Offeror must describe and identify whether or not it has any security controls, both physical and virtual Zones of Control Architectures (ZOCA), used to isolate hosted servers.

Armedia's ACC uses the AWS environment which is a virtualized, multi-tenant environment. ACC relies on AWS implemented security management processes, PCI controls, and other security controls designed to isolate each customer from other customers. ACC's use of AWS systems is designed to prevent customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software. This architecture has been validated by an independent PCI Qualified Security Assessor (QSA) and was found to be in compliance with all requirements of PCI DSS version 3.2 published in April 2016.

ACC also supports AWS single-tenancy options. Dedicated Instances are Amazon EC2 instances launched within your Amazon Virtual Private Cloud (Amazon VPC) that run hardware dedicated to a single customer. Dedicated Instances let you take full advantage of the benefits of Amazon VPC and the AWS Cloud while isolating your Amazon EC2 compute instances at the hardware level.

6.6.10 Security Technical Reference Architectures

8.6.10 Provide Security Technical Reference Architectures that support Infrastructure as a Service (IaaS), Software as a Service (SaaS) & Platform as a Service (PaaS).

The ADF is designed to be deployed in a multi-zonal ACC environment that places high value on data security (Figure 6). It uses AWS encrypted data stores providing data security at rest and uses TLS 1.2 and SSH configured using strong cipher suites for protecting the data in transit.

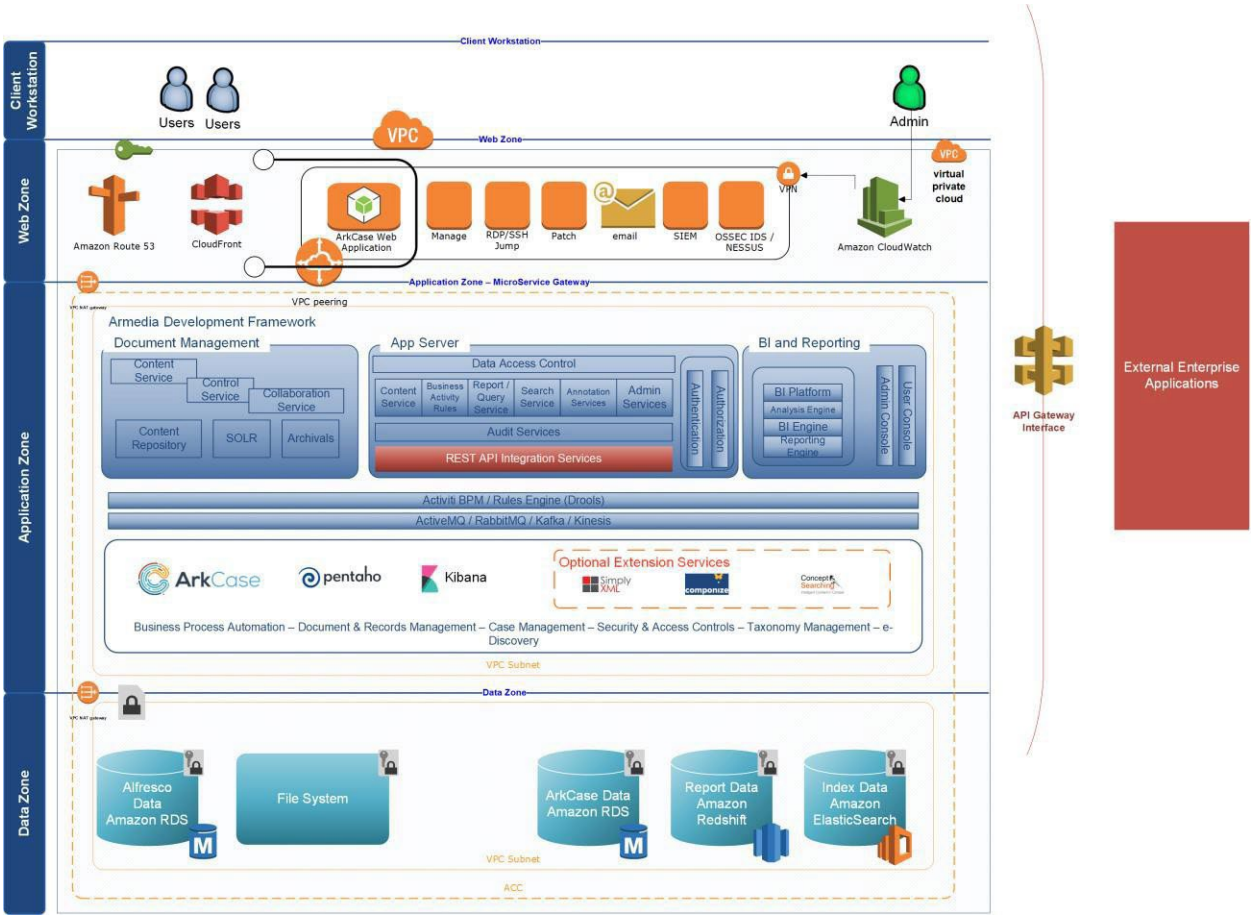


Figure 6 - Multi-zonal ADF architecture with distinct VPC subnets for data security

The architecture is comprised of a web zone, application zone, and data zone where each is separated and protected by firewalls and access policies.

- Web-zone – Hosts the web application built on Angular that facilitates user interactions with the ADF platform. This interface uses secure transport layer (HTTPS) protocols to securely transmit data between the end users and the ADF platform. The HTTPS transport layer uses trusted PKI certificates to encrypt and secure any data transmitted from the browsers to the ADF platform. The web application interface also employs a responsive design making the interface workable on desktop as well as mobile devices.
- Application Zone – Hosts multiple components of the business application based on ADF – the main ArkCase application server (a Java-Spring framework-based middleware application with Spring Security and Java cryptographic libraries), Alfresco Content Services, Alfresco Activiti business process management (BPM) components. ArkCase application provides services that includes, but are not limited to
    - Incident management module
    - Case management module
    - Document and Records management module
    - Reporting module
    - Security and role-based access controls
    - Forms module
    - Annotation and redaction module
    - Communications module

- Business rules module
- Full text-search module
- Auditing module
- Analytics and BI dashboard module
- An enterprise service bus (ESB) module

- Data Zone – Hosts the application database utilizing encrypted data stores for sensitive information, Alfresco content store (also encrypted) for storing various documents and records as it relates to the ADF application, file server for facilitating uploads of documents and virus scanning before it gets stored in the Alfresco ECM.
- External Interfaces – These are the external applications that the ADF platform will integrate with through its representational state transfer (REST) / service-oriented architecture (SOA) application programming interfaces (APIs). The known applications include FMS, NTI, SMART, HR etc. ArkCase uses ActiveMQ - the leading open source integration platform as the orchestration engine for external interfaces.

ADF multi-zonal architecture provides independent scalability at each zone for the solutions built using ADF. This approach provides granular control and configuration options on how the platform can meet growth demands.

Figure 7 depicts a sample ACC setup for ADF based application developed and maintained by Armedia for Pan-America Health Organization.

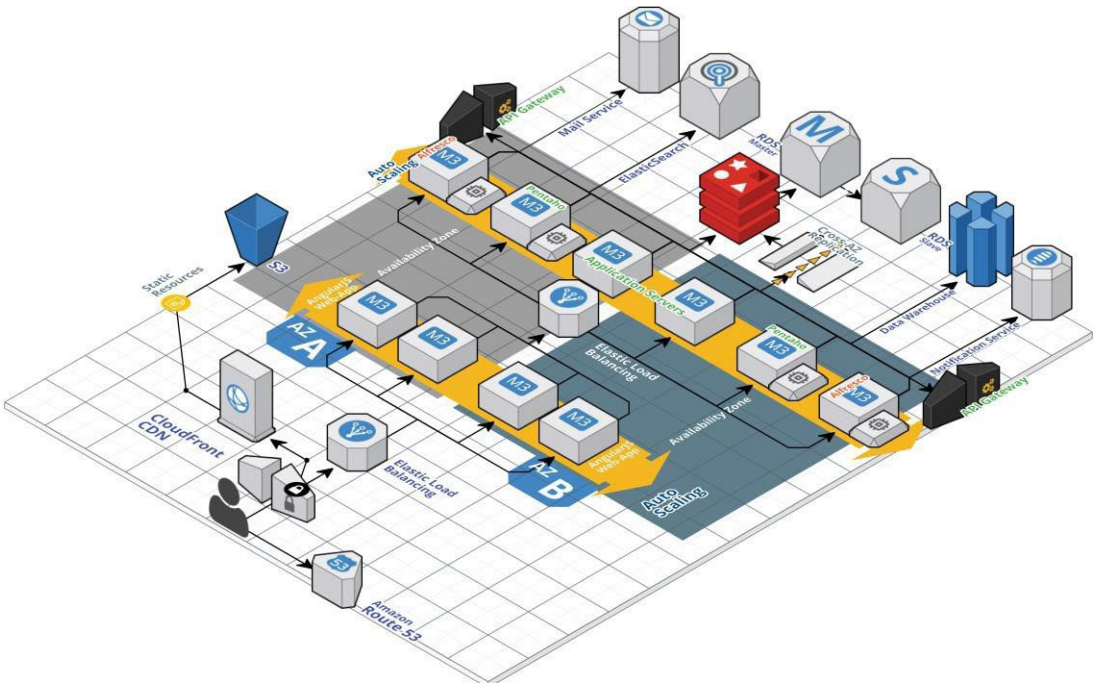


Figure 7 - ACC architecture for ADF based applications using a High-Availability, High-Scalability configuration

The Purchasing Entities retain the responsibility to create, setup and monitor their own environments that they manage for their customers. Armedia offers sample architecture recommendations for solutions created using ADF and deployed on ACC (Figure 7).

Armedia's security implementation utilizes a standardized reference architecture, in which the following functionality is deployed in all Armedia PaaS and SaaS offerings:

- Authentication and Authorization (Currently utilizing Active Directory for authentication/authorization)
- Network Protection (Currently utilizing AWS Security Groups and AWS DoS protection for network protection)
- System and Service Hardening (Currently using CIS Benchmarks and DISA STIGs as configuration baselines)
- File Integrity Monitoring (Currently utilizing OSSEC for file integrity monitoring)
- Host-based Intrusion Detection (Currently utilizing OSSEC for file integrity monitoring)
- Malware Detection/Protection (Currently utilizing Trend Micro and ClamAV for malware detection and protection)
- Log Analysis and Correlation (Currently utilizing ELK for log archiving, analysis, and correlation)
- Vulnerability Management (Currently utilizing Tenable Nessus for vulnerability detection)

6.6.11 Security Procedures for Employees

8.6.11 Describe security procedures (background checks, foot printing logging, etc.) which are in place regarding Offeror's employees who have access to sensitive data.

Armedia employees undergo successful background and drug checks prior to employment. Armedia employees do not have physical access to any of the systems, as Armedia's PaaS and SaaS offerings are entirely hosted on Amazon Web Services. Once employed, Armedia facilities are controlled by a badging system so public users cannot enter our work space. In addition, employees must authenticate to gain access to systems within the domain and once authenticated, user actions are logged for auditing.

Armedia will meet with Purchasing Entity to review our Security Procedures and if additional measures are necessary, we will implement them for employees accessing the Purchasing Entities systems and data. Armedia is accustomed to operating in this manner for our commercial and government clients with specific requirements (i.e. Top-Secret, CJIS, HIPAA, etc.)

6.6.12 Confidentiality of Data

8.6.12 Describe the security measures and standards (i.e. NIST) which the Offeror has in place to secure the confidentiality of data at rest and in transit.

Armedia utilizes encryption methods compliant with the requirements of NIST Special Publication 800-53 Rev4 and industry best practices in order to protect the confidentiality of customer information at rest and in transit. Specifically, data in transit for Armedia's PaaS and Sass offerings is protected using encryption technologies including:

- TLS (utilizing only TLS versions 1.1 and 1.2)
- SSH

Additionally, TLS and SSH are configured to only utilize strong cipher suites for the protection of information in transit.

File-level data at rest is stored on encrypted AWS EBS volumes. Database information at rest is stored in AWS RDS encrypted databases. Archived data is stored in encrypted AWS S3 buckets and AWS Glacier. All data at rest is encrypted using AWS-provided encryption methods, which utilize AES-256 encryption.

6.6.13 Notification in the Event of a Data Breach

8.6.13 Describe policies and procedures regarding notification to both the State and the Cardholders of a data breach, as defined in this RFP, and the mitigation of such a breach.

Armedia's process of notification in the event of a data breach is described in response to Privacy and Security – Notification Process.

Since the Purchasing Entities will be developing custom solutions using ADF and deploying those solutions in the ACC, the Purchasing Entities retain the responsibility to monitor their own environment for privacy breaches.

6.7 Migration and Redeployment Plan

6.7.1 Closing Down a Service

8.7.1 Offeror must describe how it manages the end of life activities of closing down a service to a Purchasing Entity and safely deprovisioning it before the Offeror is no longer contractually obligated to maintain the service, include planned and unplanned activities. An Offeror's response should include detail on how an Offeror maintains security of the data during this phase of an SLA, if the Offeror provides for redundancy during migration, and how portable the data is during migration.

Armedia is committed to working with the Purchasing Entity on closing down of a service on ACC as per the agreement with the Purchasing Entity. When Armedia is contracted to develop custom solutions on behalf of the Purchasing Entity, Armedia will provide and update the Purchasing Entity with the service closing process documentation and will transfer all the data to the Purchasing Entity and its customer as agreed in the contract. Armedia ensures total shutdown and termination of services including deleting all associated data on ACC once the data transfer is completed after service closure.

In all other cases, the Purchasing Entities manage the creation and deletion of their data on ACC, as well as maintain control of access permissions. The Purchasing Entities are responsible for maintaining appropriate data retention policies and procedures. The Purchasing Entities in place limit access to systems and data and provide that access to systems or data is restricted and monitored. In addition, customer data and server instances are logically isolated from other customers by default. Privileged user access control is reviewed by an independent auditor during the AWS SOC 1, ISO 27001, PCI, and FedRAMP audits.

6.7.2 The Return of Data

8.7.2 Offeror must describe how it intends to provide an orderly return of data back to the Purchasing Entity, include any description in your SLA that describes the return of data to a customer.

In the case where Armedia is contracted to develop custom solutions using ADF and ACC on behalf of the Purchasing Entity, Armedia agrees to return all data back to the Purchasing Entity using AWS Import/Export Disk and AWS Snowball Edge service to ensure secure data transfer. Transferring data with AWS Import/Export Disk and AWS Snowball Edge is simple, fast, more secure, and can be as little as one-fifth the cost of transferring data via high-speed Internet.

In all other cases, the Purchasing Entities are responsible for managing their data.

6.8 Service or Data Recovery

8.8.1 Describe how you would respond to the following situations; include any contingency plan or policy.
a. Extended downtime.
b. Suffers an unrecoverable loss of data.
c. Offeror experiences a system failure.
d. Ability to recover and restore data within 4 business hours in the event of a severe system outage.
e. Describe your Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

ACC uses Amazon's infrastructure that has a high level of availability and provides customers the features to deploy a resilient IT architecture. Armedia has designed its ACC systems to tolerate system or hardware failures with minimal customer impact.

6.8.1 a. Extended Downtime

ACC is architected and designed to take advantage of multiple AWS regions and AWS availability zones (Figure 7). Distributing applications across multiple availability zones provides the ability to remain resilient in the face of most failure modes, including natural disasters or system failures.

6.8.2 b. Loss of Data

ACC's use of AWS infrastructure taking advantage of multiple AWS regions and availability zones provides resilience to loss of data due to system failure through having copies of data across regions and availability zones. ACC also creates periodic backup snapshots of the system that can be used for recovery of data.

Additionally, when contracted to develop solutions on behalf of the Purchasing Entity using ADF and ACC, Armedia provides the option of using a disaster recovery (DR) setup along with the high-availability, high-resilient setup for its solutions at an additional service cost to the Purchasing Entity. Armedia takes full responsibility of maintaining the data copies at the DR with snapshots of data and the applications taken at regular intervals in a manner that would minimize unrecoverable loss of data.

In all other cases, the Purchasing Entities are responsible for protecting against unrecoverable loss of data through their own DR and data recovery mechanisms.

6.8.3 c. System Failures

ACC is guaranteed by the AWS infrastructure SLAs that account for any system failures.

6.8.4 d. Data Recovery

The time of data recovery varies and is dependent on the total volume of data being recovered as well as the method of data recovery – recovery from a passive DR instance (shorter recovery time) vs recovery from cold backups (longer recovery time).

6.8.5 e. RPO and RTO

The design and implementation of ACC will support the requirements related to recoverability as they pertain to with an RPO of 0 to 4 hours and a RTO of 0 to 8 hours

6.8.6 Backup and Restore Services

8.8.2 Describe your methodologies for the following backup and restore services:
a. Method of data backups
b. Method of server image backups
c. Digital location of backup storage (secondary storage, tape, etc.)
d. Alternate data center strategies for primary data centers within the continental United States

When contracted to develop solutions on behalf of the Purchasing Entity using ADF and ACC, Armedia provides the option of using a disaster recovery (DR) setup along with the high-availability, high-resilient setup for its solutions at an additional service cost to the Purchasing Entity. Armedia takes full responsibility of maintaining the data copies at the DR with syncing of data and the applications at regular intervals in a manner that would minimize unrecoverable loss of data.

ACC also creates backup of data stored on AWS EBS by taking point-in-time snapshots that can be used to restore data in case of a disk volume failure.

Purchasing entities have options to create DR sites using different AWS regions – geographically separated across the globe based on the data retention and management policies. AWS currently has 18 regions, 54 Availability Zones, and 1 Local Region throughout the world: US East (Northern Virginia), US East (Ohio), US West (Oregon), US West (Northern California), AWS GovCloud (US-West), Canada (Central), EU (Ireland), EU (Frankfurt), EU (London), EU (Paris), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), Asia Pacific (Seoul), Asia Pacific (Mumbai), Asia Pacific (Osaka-Local), South America (Sao Paulo), China (Beijing), and China (Ningxia). Information on each region can be found at the AWS Global Infrastructure webpage.

6.9 Data Protection

6.9.1 Methodology

8.9.1 Specify standard encryption technologies and options to protect sensitive data, depending on the particular service model that you intend to provide under this Master Agreement, while in transit or at rest.

Securing Data at Rest

ACC and ADF support multiple options for encrypting data at rest, ranging from completely automated encryption solutions (using AWS Key Management Service [KMS]) to manual, client-side options (using AWS CloudHSM). The Purchasing Entity can choose the option based on the customer requirements for key management.

Securing Data in Transit

Protecting data in transit when running applications in the cloud involves protecting network traffic between clients and servers and network traffic between servers.

ACC provides support for both Internet Protocol Security (IPSec) and Secure Sockets Layer/Transport Layer Security (SSL/TLS) for protection of data in transit. IPSec is a protocol that extends the IP protocol stack, often in network infrastructure, and allows applications on upper layers to communicate securely without modification. SSL/TLS, on the other hand, operates at the session layer, and while there are third-party SSL/TLS wrappers, it often requires support at the application layer as well.

6.9.2 Business Associate Agreement

8.9.2 Describe whether or not it is willing to sign relevant and applicable Business Associate Agreement or any other agreement that may be necessary to protect data with a Purchasing Entity.

Armedia agrees and is willing to sign relevant and applicable Business Associate Agreements or any other agreement that may be necessary to protect data with a Purchasing Entity.

6.9.3 Data Usage

8.9.3 Offeror must describe how it will only use data for purposes defined in the Master Agreement, participating addendum, or related service level agreement. Offeror shall not use the government data or government related data for any other purpose including but not limited to data mining. Offeror or its subcontractors shall not resell nor otherwise redistribute information gained from its access to the data received as a result of this RFP.

Armedia does not access or use customer content for any purpose other than as legally required and to provide the ACC and ADF services selected by each customer, to that customer and its end users. Armedia never uses customer content or derives information from it for other purposes such as marketing or advertising. Armedia will only use NASPO customer data for purposes defined in the Master Agreement, participating addendum, or related service level agreement. Armedia does not resell or redistribute customer information, and does not use customer information for data mining purposes.

6.10 Service Level Agreements

The ACC infrastructure is backed by the underlying AWS infrastructure on which it is built and thereby is supported by the AWS SLAs for its services.

Additionally, Armedia offers SLAs for the platforms deployed and configured on the ACC as part of the ADF components which is described below. Please refer to information provided in section 6.10.2.

6.10.1 Negotiability

8.10.1 Offeror must describe whether your sample Service Level Agreement is negotiable. If not describe how it benefits purchasing entity's not to negotiate your Service Level Agreement.

Armedia provides the flexibility with our Service Level Agreement (SLA) to accommodate our customers' constraints.

6.10.2 Sample of a Service Level Agreement

8.10.2 Offeror, as part of its proposal, must provide a sample of its Service Level Agreement, which should define the performance and other operating parameters within which the infrastructure must operate to meet IT System and Purchasing Entity's requirements.

6.11 Service Level Agreement

Armedia's Service Level Agreement (SLA) makes Services available with a Monthly Uptime Percentage (defined below) of at least 99.9%, in each case during any monthly billing cycle (the "Service Commitment"). In the event Services do not meet the Service Commitment, the Purchasing Entity will be eligible to receive a Service Credit as described below. Armedia will issue a monthly report with Monthly Uptime Percentages and outlining issues or factors discussed in this SLA to provide greater understanding to the Purchasing Entity. ("SLA Reports")

Definitions
"**Monthly Uptime Percentage**" is calculated by subtracting from 100% the percentage of minutes during the month in which Services, as applicable, was in the state of "Region Unavailable" or "Unavailable". Monthly Uptime Percentage measurements exclude downtime resulting directly or indirectly from any Services SLA Exclusion (defined below).
"**Region Unavailable**" and "**Region Unavailability**" mean that more than one Availability Zone in which you are running an instance, within the same Region, is "**Unavailable**" to you.
"**Unavailable**" and "**Unavailability**" for Services is when all of your running instances have no external connectivity, or any material features of the Service are not operating in accordance with the Agreement, including the Response Time Commitment.
A "**Service Credit**" is a dollar credit, calculated as set forth below, that we may credit back to an eligible account.

Service Commitments and Service Credits
Service Credits are calculated as a percentage of the monthly charges paid by Purchasing Entity (excluding one-time payments) for Services (which were Unavailable) in the Region affected for the monthly billing cycle in which the Region Unavailability occurred in accordance with the schedule below.

Table 1 Monthly Uptime and Service Credit Percentage:

Monthly Uptime Percentage	Monthly Service Credit Percentage
Less than 98.0%	10%
Less than 95.0%	20%

We will apply any Service Credits only against future Services payments otherwise due from Purchasing Entity. A Service Credit will be applicable and issued only if the credit amount for the applicable monthly billing cycle is greater than one dollar ($1 USD). Service Credits may not be transferred or applied to any other account.

Credit Procedures
Armedia will issue Service Credits based on the SLA Reports on the next monthly invoice.

Armedia Services SLA Exclusions
The Service Commitment does not apply to any unavailability, suspension or termination of Services, or any other Services performance issues: (i) that result from a suspension of Services; (ii) caused by factors outside of our reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Services; (iii) that result from any actions or inactions of you or any third party; (iv) that result from your equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment, software or other technology within our direct control); (v) that result from failures of individual instances or volumes not attributable to Region Unavailability; (vi) that result from any maintenance as provided for pursuant to the Agreement; or (vii) arising from our ` and termination of your right to use Services in accordance with the Agreement (collectively, the "**Armedia Services SLA Exclusions**"). If availability is impacted by factors other than those used in our Monthly Uptime Percentage calculation, then we may issue a Service Credit considering such factors at our discretion.

Notifications
Armedia will develop a Communications Plan to govern the project; however, the table below defines the SLAs for notifying Purchasing Entity.

Table 2 Notifications

Incident Category	Notifier	Notification SLA to the Purchasing Entity	Notification SLA to Impacted Parties
Security breaches, compromise of PII data, and corruption of data	Armedia PM	Immediately and daily until a full understanding of the spillage and a consensus to stop reporting	Armedia will work with Purchasing Entity to draft a formal communication with the appropriate mitigations/remedies (i.e. credit monitoring)
Outages (RPO, RTO)	Armedia PM	Immediately and hourly until Services are operational	Immediately via website
Any other required notification	Armedia PM	As defined by the Communications Plan	As defined by the Communications Plan

Measuring SLA Performance
Armedia will provide a Service Report each month that identifies our adherence to the SLA. Each SLA criteria will be monitored and measured for compliance by Purchasing Entity.

SLA Enforcement Mechanisms
Armedia will provide a Service Report each month that identifies our adherence to the SLA. If Service Credits are warranted based on Table 1, Armedia will identify the Service Credits and how they will be applied to the next monthly invoice. If the Purchasing Entity disagrees with the Service Report, Armedia will work with the Purchasing Entity to come to consensus and apply the appropriate Service Credit if deem required.

Service Monitoring
Armedia will provide a Service Report each month that identifies our adherence to the SLA. Each SLA criteria will be monitored and measured daily of which the daily metrics will be compiled and presented in the report.

6.12 Data Disposal

8.11 Specify your data disposal procedures and policies and destruction confirmation process.

Armedia provides customers with the ability to delete their data. The Purchasing Entities retain control and ownership of their data, and it is the Purchasing Entity's responsibility to manage their data.

ACC uses AWS encrypted storage devices for storing the data and the data disposition during device decommissioning utilizes AWS data device decommissioning procedures that are designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.

6.13 Performance measures and Reporting

6.13.1 Reliability and Uptime

8.12.1 Describe your ability to guarantee reliability and uptime greater than 99.5%. Additional points will be awarded for 99.9% or greater availability.

Armedia offers a 99.9% availability of ACC. For applications developed by the Purchasing Entity using ADF, the reliability and uptime guarantee will need to be provided by the Purchasing Entity. Armedia is committed to supporting the Purchasing Entities for any issues with ADF pursuant to the terms of the purchased support service.

6.13.2 SLA Criteria

8.12.2 Provide your standard uptime service and related Service Level Agreement (SLA) criteria.

ACC is backed by SLA guarantees of AWS on which it is based. AWS offers SLAs for services such as Amazon EC2 and Amazon EBS at 99.9%, and Amazon S3 with an SLA of 99.9%.

Armedia will provide a Service Report each month that identifies our adherence to the SLA. Each SLA criteria will be monitored and measured daily for which graphical reports will be presented to the Purchasing Entity and its customers.

6.13.3 End User Support

8.12.3 Specify and provide the process to be used for the participating entity to call/contact you for support, who will be providing the support, and describe the basis of availability.

The Armedia Customer Support Team will respond to tickets/requests 24 hours per day, 7 days a week (24x7). Table 3 defines severity class level response timeframes, effort required until resolution, and update frequencies currently employed by Armedia Customer Support Team:

Table 3 - Standard Support Response Time

Severity Class	Initial Response to Customer	Effort Required Until Resolution	Update Frequencies
Class 1	No greater than two hours if reported during normal business hours. Errors reported other times will receive a response on the next normal business day.	Constant effort during normal business hours until relief is provided in the form of a Work-Around or a software hotfix.	As mutually agreed but at a minimum, every business day during normal business hours via conference call or at Armedia's registered business location unless both Parties have agreed to a different frequency and location.
Class 2	Next business day but no greater than 24 hours.	Commercially reasonable efforts during normal business hours until there is a Work-Around or Call Remedy in the form of a software hotfix or service pack	As mutually agreed but at a minimum, Customer may request a summary report of all Severity 2 issues a maximum of once every five business days unless both Parties have agreed to a different frequency. Summary reports may be conveyed in e-mail format or verbally.
Class 3	No greater than five business days	Does not require immediate action. Normally addressed in a service pack at Armedia's sole discretion.	As mutually agreed but at a minimum, Customer may request a summary report of all Severity 3 issues a maximum of once per calendar month or per mutually agreed action plan.

Operations Management. The Armedia Operations Team will have a dedicated Project Manager who will oversee operational tasks such as system enhancements, problem resolution, change requests, system deployment and system performance inquiries.

Armedia will develop a Communications Plan to govern the project; however, Table 4 Notifications defines the SLAs for notifying the Purchasing Entity and its customers

Table 4 Notifications

Incident Category	Point of Contact	Notification SLA to the Purchasing Entity	Notification SLA to Impacted Parties
Security breaches, compromise of PII data, and corruption of data	Armedia PM	Immediately and daily until a full understanding of the spillage and a consensus to stop reporting	Armedia will work with Purchasing Entity to draft a formal communication with the appropriate mitigations/remedies (i.e. credit monitoring)
Outages (RPO, RTO)	Armedia PM	Immediately and hourly until Services are operational	Immediately via website
Any other required notification	Armedia PM	As defined by the Communications Plan	As defined by the Communications Plan

6.13.4 SLA Remedies

8.12.4 Describe the consequences/SLA remedies if the Respondent fails to meet incident response time and incident fix time.

Service Credits are calculated as a percentage of the total charges paid by the Purchasing Entity and its customers and (excluding one-time payments) for Services (which were Unavailable) in the Region affected for the monthly billing cycle in which the Region Unavailability occurred in accordance with the schedule below.

Table 5 - Monthly Uptime and Service Credit Percentage

Monthly Uptime Percentage	Monthly Service Credit Percentage
Less than 98.0%	10%
Less than 95.0%	20%

We will apply any Service Credits only against future Services payments otherwise due from the Purchasing Entity. A Service Credit will be applicable and issued only if the credit amount for the applicable monthly billing cycle is greater than one dollar ($1 USD). Service Credits may not be transferred or applied to any other account.

6.13.5 Planned Downtime Procedures

8.12.5 Describe the firm's procedures and schedules for any planned downtime.

ACC does not require systems to be brought offline to perform regular maintenance and system patching, and AWS's own maintenance and system patching generally do not impact customers. There may be occasions when AWS might schedule a customer instance for a reboot for necessary maintenance, such as to apply updates that require a reboot. Armedia will communicate with the Purchasing Entity and its customers of any such known reboots. No action is required on the customer's part; we recommend that customers wait for the reboot to occur within its scheduled window. These scheduled events are not frequent and if a customer instance will be affected by a scheduled event, they will receive an email prior to the scheduled event with details about the event, as well as a start and end date. Customers can also view scheduled events for their instance(s) by using the Amazon EC2 Console, API, or CLI. AWS will communicate with customers, either via email, or through the AWS Service Health Dashboard if service use is likely to be adversely affected.

Besides these, the Purchasing Entities and their customers may incur a scheduled downtime for any application component upgrades on ACC. The Purchasing Entity would be responsible for such upgrades and its associated downtimes and would also be responsible in communicating that with their customers.

6.13.6 Disaster Recovery SLA Remedies

8.12.6 Describe the consequences/SLA remedies if disaster recovery metrics are not met.

Please refer to SLA Remedies.

6.13.7 Performance Reports

8.12.7 Provide a sample of performance reports and specify if they are available over the Web and if they are real-time statistics or batch statistics.
8.12.8 Ability to print historical, statistical, and usage reports locally.

Measuring SLA Performance

Armedia will provide a Service Report each month that identifies our adherence to the SLA. Each SLA criteria will be monitored and measured daily for which graphical reports will be presented to the Purchasing Entity and its customers. Purchasing Entities have the option of setting up role-based access controlled dynamic dashboards for real-time statistics (Figure 8).

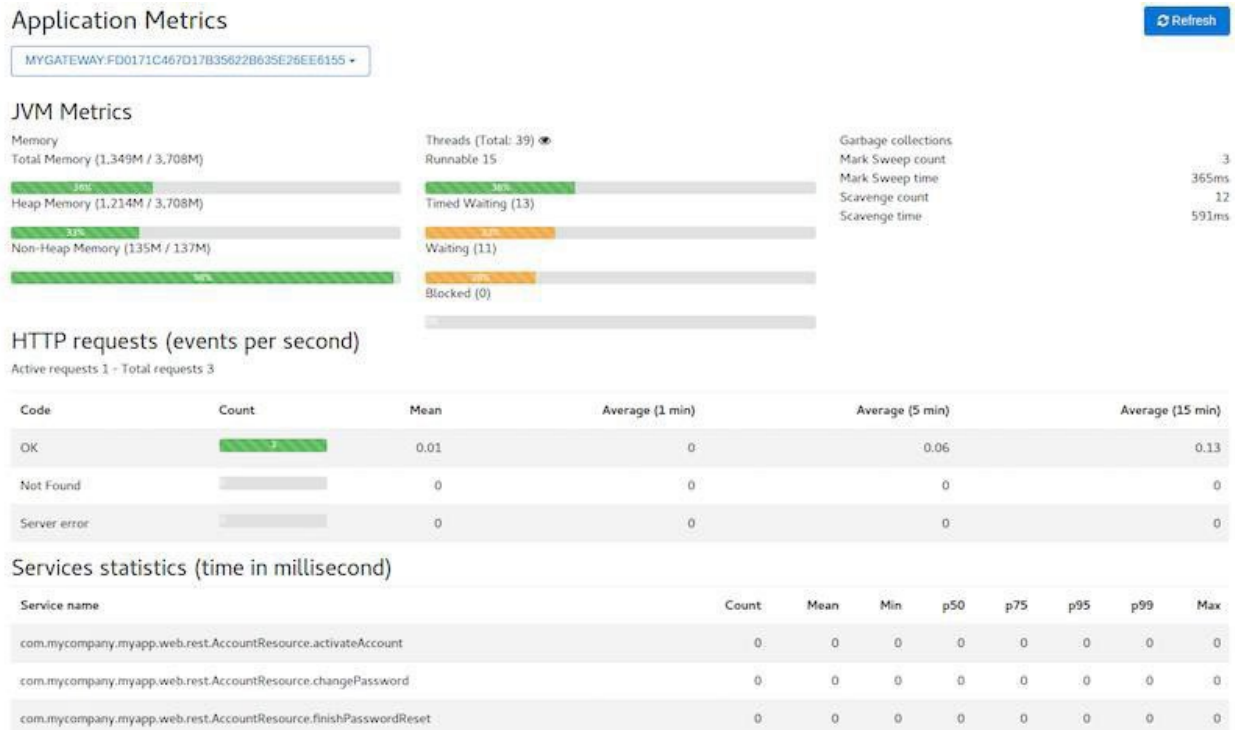


Figure 8 - ADF and ACC Key Performance Indicator Metrics Dashboard for real time statistics

SLA Enforcement Mechanisms

Armedia will provide a Service Report each month that identifies our adherence to the SLA. If Service Credits are warranted based on Table 5, Armedia will identify the Service Credits and how they will be applied to the next monthly invoice. If the Purchasing Entity disagrees with the Service Report, Armedia will work with the Purchasing Entity to come to consensus and apply the appropriate Service Credit if deem required.

Service Monitoring

Armedia will provide a Service Report each month that identifies our adherence to the SLA (Figure 9). Each SLA criteria will be monitored and measured daily of which the daily metrics will be compiled and presented in the report.

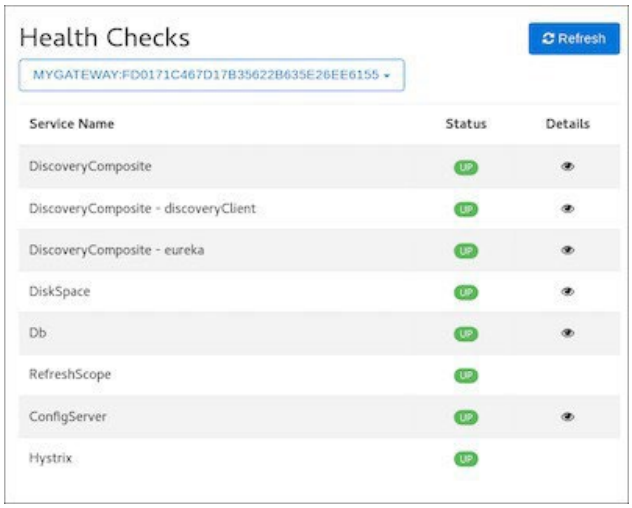


Figure 9 - ACC Health Check Dashboard for service monitoring

6.13.8 On-Demand Deployment and Scalability

8.12.9 Offeror must describe whether or not its on-demand deployment is supported 24x365.
8.12.10 Offeror must describe its scale-up and scale-down, and whether it is available 24x365.

ACC makes use of AWS auto scaling that allows the Purchasing Entities to automatically scale their ACC capacity up or down according to conditions that they define (Figure 7). Auto Scaling is well suited for applications that experience hourly, daily, or weekly variability in usage. Customers can automatically scale their ACC fleet or maintain their ACC fleet at a set size.

Auto Scaling enables customers to closely follow the demand curve for their applications, reducing the need to provision ACC capacity in advance. For example, customers can set a condition to add new ACC instances in increments of three instances to the Auto Scaling Group when the average CPU utilization of the ACC fleet goes above 70%; and similarly, customers can set a condition to remove ACC instances in the same increments when CPU utilization falls below 10%.

Often, customers may want more time to allow their fleet to stabilize before Auto Scaling adds or removes more Amazon EC2 instances. Customers can configure a cool down period for their Auto Scaling Group, which tells Auto Scaling to wait for some time after taking an action before it evaluates the conditions again. Auto Scaling enables customers to run their Amazon EC2 fleet at optimal utilization.

Elastic Load Balancing

ACC also uses Elastic Load Balancing that automatically distributes incoming application traffic across multiple Amazon EC2 instances. It enables Purchasing Entity to achieve even greater fault tolerance in their applications, seamlessly providing the amount of load balancing capacity needed in response to incoming application traffic. Elastic Load Balancing detects unhealthy instances and automatically reroutes traffic to healthy instances until the unhealthy instances have been restored. Purchasing Entity can enable Elastic Load Balancing within a single Availability Zone or across multiple zones for even more consistent application performance (Figure 7).

6.14 Cloud Security Alliance

Describe and provide your level of disclosure with CSA Star Registry for each Solution offered.

a. Completion of a CSA STAR Self-Assessment. (3 points)
b. Completion of Exhibits 1 and 2 to Attachment B. (3 points)
c. Completion of a CSA STAR Attestation, Certification, or Assessment. (4 points)
d. Completion CSA STAR Continuous Monitoring. (5 points)

A CSA STAR Self-Assessment has been completed for Armedia's PaaS and SaaS offerings, and the CSA STAR CAIQ is attached. Please refer the response to section 8.6.2

6.15 Service Provisioning

6.15.1 Surge Support

8.14.1 Describe in detail how your firm processes emergency or rush services implementation requests by a Purchasing Entity.
8.14.2 Describe in detail the standard lead-time for provisioning your Solutions.

ACC uses AWS auto-scaling that provides the ability to scale computing resources up and down easily, with minimal friction. This elasticity helps you avoid provisioning resources up front for projects with variable consumption rates or short lifetimes. Instead of acquiring hardware, setting it up, and maintaining it in order to allocate resources to your applications, you use AWS to allocate resources using simple API calls. Elastic Load Balancing and Auto Scaling can automatically scale your AWS cloud-based resources up to meet unexpected demand, and then scale those resources down as demand decreases.

6.16 Back up and Disaster Plan

6.16.1 Legal Retention Periods

8.15.1 Ability to apply legal retention periods and disposition by agency per purchasing entity policy and/or legal requirements.

The Purchasing Entities control the entire life-cycle of their content on ACC and manage their content in accordance with their own specific needs, including content classification, access control, retention and deletion.

6.16.2 Mitigation Strategies

8.15.2 Describe any known inherent disaster recovery risks and provide potential mitigation strategies.

The ACC infrastructure has a high level of availability and we provide you with the features you need to deploy a resilient IT architecture. Our systems are designed to tolerate system or hardware failures with minimal customer impact. ACC supports many popular disaster recovery architectures, ranging from “pilot light” environments that are ready to scale up at a moment’s notice to “hot standby” environments that enable rapid failover.

All data centers are online and serving customers; no data center is “cold.” In the case of a failure, automated processes move your data traffic away from the affected area. By distributing applications across multiple AWS Availability Zones, you can remain resilient in the face of most failure modes, including natural disasters or system failures. You can build highly resilient systems in the cloud by employing multiple instances in multiple AWS Availability Zones and using data replication to achieve extremely high recovery time and recovery point objectives.

The Purchasing Entities are responsible for managing and testing the backup and recovery of their information system that is built on the ACC infrastructure. You can use the ACC infrastructure to enable faster disaster recovery of your critical IT systems without incurring the infrastructure expense of a second physical site.

6.16.3 The Support of Multiple Data Centers

8.15.3 Describe the infrastructure that supports multiple data centers within the United States, each of which supports redundancy, failover capability, and the ability to run large scale applications independently in case one data center is lost.

ACC relies on the AWS data centers for its infrastructure setup. The AWS Cloud infrastructure is built around regions and Availability Zones. A region is a physical location in the world where we have multiple Availability Zones. Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity and housed in separate facilities. These Availability Zones offer customers the ability to operate production applications and databases that are more highly available, fault tolerant, and scalable than would be possible with a single data center.

ACC can be setup using any combination of the AWS's 18 regions, 54 Availability Zones, and 1 Local Region throughout the world: US East (Northern Virginia), US East (Ohio), US West (Oregon), US West (Northern California), AWS GovCloud (US-West), Canada (Central), EU (Ireland), EU (Frankfurt), EU (London), EU (Paris), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), Asia Pacific (Seoul), Asia Pacific (Mumbai), Asia Pacific (Osaka-Local), South America (Sao Paulo), China (Beijing), and China (Ningxia).

6.17 Hosting and Provisioning

6.17.1 Cloud Hosting Provisioning Process

8.16.1 Documented cloud hosting provisioning processes, and your defined/standard cloud provisioning stack.

The ACC infrastructure can be controlled using the AWS Management Console which is a single destination for managing all AWS resources, from Amazon Elastic Compute Cloud (Amazon EC2) instances to Amazon DynamoDB tables. Purchasing Entities can use the AWS Management Console to perform any number of tasks, from deploying new applications to monitoring the health of applications. The AWS Management Console also enables customers to manage all aspects of their AWS account, including accessing monthly spending by service, managing security credentials, or even setting up new AWS Identity and Access Management (AWS IAM) users. The AWS Management Console supports all AWS Regions and lets customers provision resources across multiple regions.

6.17.2 Tool Sets

Provide tool sets at minimum for:
1. *Deploying new servers (determining configuration for both stand alone or part of an existing server farm, etc.)*
2. *Creating and storing server images for future multiple deployments*

The ACC uses the AWS management console to configure servers required for its business process automation offerings that includes ArkCase – the Armedia SaaS offering for case management. ACC also uses a range of supporting components like management tools, networking services, and application augmentation services, with multiple interfaces to AWS Application Programming Interface (API)-based services, including Software Development Kits (SDKs), Integrated Development Environment (IDE) toolkits, and Command Line Tools.

3. Securing additional storage space

ACC uses AWS encrypted elastic block storage (EBS) and AWS elastic file system (EFS) for securely storing data. Amazon Elastic Block Store (Amazon EBS) provides block-level storage volumes for use with Amazon EC2 instances. Amazon EBS volumes are highly available and reliable storage volumes that can be attached to any running instance that is in the same Availability Zone. Amazon EBS volumes that are attached to an Amazon EC2 instance are exposed as storage volumes that persist independently from the life of the instance.

Amazon Elastic File System (Amazon EFS) provides simple, scalable file storage for use with Amazon EC2 instances in the AWS Cloud. Amazon EFS is easy to use and offers a simple interface that allows customers to create and configure file systems quickly and easily. With Amazon EFS, storage capacity is elastic, growing and shrinking automatically as files are added and removed, so applications have the storage they need, when they need it. Amazon EFS also allows customers to access file data from on-premises data centers. On-premises servers can move file data to and from an Amazon EFS file system when connected to an Amazon VPC with AWS Direct Connect, allowing customers to migrate data sets to Amazon EFS, enable cloud bursting scenarios, or back up on-premises data to Amazon EFS.

ACC uses AWS Import/Export Disk that accelerates moving large amounts of data into and out of the AWS cloud using portable storage devices for transport. AWS Import/Export Disk transfers data directly onto and off of storage devices using Amazon's high-speed internal network and bypassing the Internet. For significant data sets, AWS Import/Export Disk is often faster than Internet transfer and more cost effective than upgrading connectivity.

4. Monitoring tools for use by each jurisdiction's authorized personnel – and this should ideally cover components of a public (respondent hosted) or hybrid cloud (including Participating entity resources).

ACC monitoring is available for authorized personnel through the AWS management console which the Purchasing Entity can control through role-based access controls configured using the AWS identity management (IM).

6.18 Trial and Testing Periods (Pre- AND Post-Purchase)

6.18.1 Testing and Training Periods

8.17.1 Describe your testing and training periods that your offer for your service offerings.

Armedia uses test driven development for ArkCase as well as all the ADF services and components. The test results and the test coverage reports are published with every ADF release along with the release notes and are available to the Purchasing Entity.

6.18.2 Proof of Concept Environment

8.17.2 Describe how you intend to provide a test and/or proof of concept environment for evaluation that verifies your ability to meet mandatory requirements.

In collaboration with AWS, Armedia will provide test and proof of concept environments via Amazon Test Drive. Through Amazon Test Drive, Purchasing Entities will be able to spin up an environment and test drive the solution.

6.18.3 Training and Support

8.17.3 Offeror must describe what training and support it provides at no additional cost.

Armedia provides online training and videos at no additional cost via our website.

6.19 Integration and Customization

6.19.1 Integration

8.18.1 Describe how the Solutions you provide can be integrated to other complementary applications, and if you offer standard-based interface to enable additional integrations.

ADF uses a modular microservice-based architecture that uses REST APIs to loosely couple all the services (Figure 6). These REST APIs can be easily used to integrate with other complementary applications.

Based on the client demands, Armedia continuously researches and develops additional extension services for ADF that are available to customers as add-on options.

The ADF core is a Java/Spring framework-based application that ties together all the core services like document management, workflow management, security, auditing and reporting, etc., while providing a way to plug-in extension services through the micro-service architecture. **Optional** Service Extensions to the ADF platform include, but are not limited to

- **Multi-factor authentication** (MFA) service extension developed for Pan-America Health Organization (PAHO) implementation ties the Okta multi-factor authentication platform into the ArkCase implementation for PAHO. This module also supports Ping MFA as an alternative. Additional MFA platform extensions can also be configured and supported through this extension.
- **Video/Audio transcription** service extension provides the ability to transcribe video and audio files to text and provide full text search capabilities on the video and audio files stored in the underlying content management system.
- **AWS Cloud service** extension adds the ability to make use of multiple AWS cloud services – the AWS transcription service being one of those. This adds the ability to use AWS storage (S3, Glacier) and AWS data analytics services as well as AWS data warehouse (RedShift) for the ArkCase platform as needed.
- **Advanced Data Analytics** extension allows ADF platform to use either the ElasticSearch-Logstash-Kibana (ELK) or the Solr-Logstash-Kibana (SiLK) platform stacks as the data analysis and visualization platform.

6.19.2 Customization

8.18.2 Describe the ways to customize and personalize the Solutions you provide to meet the needs of specific Purchasing Entities.

Purchasing Entities can follow the same plug-n-play service architecture and develop customers' business logic as service extensions to the platform. This will enable the Purchasing Entity's customers to receive platform and component updates (updates for ArkCase core, Alfresco, Ephesoft etc.) without disrupting the business functionality of the customer.

6.20 Marketing Plan

Established in 2002 and operating out of Vienna, VA, Armedia, Inc. is a registered Veteran Owned Small Business and Minority Business Enterprise with verifiable success achieving more than $15M in annual revenue and consistent business growth. The company is building significant qualifications in Cloud Services, including a PaaS offering, the Armedia Development Framework. In addition, Armedia offers a comprehensive suite of information technology services to enhance its PaaS offering. These include ArkCase, a SaaS offering; deployment and migration services; data analytics; and technical advisory services to assist our customers in accessing the benefits of the Cloud. Shortly after Armedia was established, the company obtained subcontracts and prime contracts managing, securing, enhancing and optimizing numerous mission-critical applications for Federal agencies such as the Department of Justice (DoJ), Federal Bureau of Investigations (FBI), and commercial clients such as Delta Airlines and Purchasing Entity. Armedia continues to expand its service to the federal government providing cloud-centric services to the Postal Regulatory Commission (PRC), Pan American Health Organization (PAHO), and the US Department of Agriculture (USDA) Food and Nutrition Services (FNS). At the state and local level, Armedia provides IT support services, including cloud-oriented services, to Martin County in FL, Orange County FL, and New York State.

In 2012, Armedia was awarded a 5-year BPA by the USDA FNS for providing electronic content management services. Three years later, Armedia was awarded another 5-year BPA for six times the previous value, since that award we have introduced FNS to the Cloud, leveraging the Alfresco Content Management System and resulting in increased cost effectiveness and efficiency for their electronic content management. This contract has grown by $24.5M, which is a testament to the success that Armedia has been able to foster.

In 2017, the Pan-American Health Organization (PAHO) awarded a contract to Armedia to develop and implement a platform, the Regulatory Exchange Platform – secure (REPs), to facilitate the exchange of confidential/non-public information as well as the collaboration of global regulators in a secure IT environment. This is an international effort with initial participants including Australia, Brazil, Canada, Japan and the US. Additional countries are anticipated to join the effort soon. This platform will disseminate critical audit information on medical devices, enabling member countries to access inspection results with confidence and accuracy.

Armedia also won the contract to support the Postal Regulatory Commission (PRC) for the development of a cloud solution for their Electronic Document and Records Management System (EDRMS) which will be integrated with existing Commission systems such as email, intranet and extranet as well as replace the Commission's current Docket Management System (webDockets). PRC takes advantage of ArkCase's modular architecture which drives configuration versus

customization, an important PRC requirement to avoid costly annual system upgrades and enhancements. Armedia's ArkCase serves as the basis for the PRC cloud solution (SaaS), hosted in AWS FedRAMP PaaS. In partnership with Armedia, PRC is the agency sponsor for Armedia to attain the FedRAMP Agency Path Authorization.

In addition to replacing PRC's legacy Docket Management System, Armedia will provide a Freedom of Information Act (FOIA) module in the next phase of the project, to be hosted on our FedRAMP PaaS.

Recognizing that the government's cloud market will be worth an estimated $28.85 Billion USD by 2022, Armedia is investing heavily in both its PaaS and SaaS cloud offerings through research and development efforts, personnel training, partnerships development and marketing. Starting in 2015, the company developed an aggressive, multi-year growth plan, investing over $2M for this purpose. This initiative included hiring additional development personnel focused on R&D and cloud infrastructure, as well as expanding the dedicated business development division to bring in individuals tasked with marketing Armedia's services and capabilities to targeted audiences, and dedicated time and effort to the development of the cloud business at the state and federal government levels. Our team is multifunctional and includes delivery, operations and business development professionals; each providing guidance and advice in their particular areas of expertise. In support of this growth initiative, Armedia has invested in capture and proposal tools, enterprise infrastructure, digital marketing, brand awareness, and dedicated recruiting capability.

Situation Analysis

Armedia's Current Situation

Armedia developed the majority of its experience through prime awarded contracts on GSA Schedule 70 and on the open market. In addition, Armedia has been brought onto projects in a sub-contract arrangement by large systems integrators. Armedia continues to market aggressively to state businesses through its Schedule 70 GWAC and in open market solicitations. With the award of NASPO, Armedia will continue to market to our state business, recommending the use of the NASPO ValuePoint (NVP) Cloud Solution as a preferred avenue for placing business. We recognize that the NASPO Master Agreement offers strong value to state procurement initiatives in that it is flexible and efficient in terms of cost and time.

Market Trends

Government CIOs view the Cloud as a key practice to enable Information Technology to address the larger transformative shifts that are allowing them to better meet their agency's goals. Armedia has identified several market needs:

- Identifying challenges that government agencies face when procuring and adopting cloud technologies,
- Aligning FISMA and IT security with cloud-based hosting
- Assisting agencies in making the transition to a cloud-based environment
- Migration to the cloud-based services
- Legacy modernization, using cloud infrastructure

SWOT Analysis

Strengths

- Company's reputation and performance
- Long term clients and relationships
- Experienced professionals with federal, state and local government, and commercial experience

- Key government clients – USDA, DOD, Senate, FDA, PAHO and PRC
- Strong management emphasis on Cloud as a growth mechanism
- Continuous investing in R&D to enhance both the PaaS and SaaS offering
- Development in staff to support the growth goals through training and certifications indicating a long-term, strategic approach
- Investing in certifications such as CMMI Dev level 3 and ISO 9001.
- Competitive rates and low overhead contribute to a nimble approach toward our customers' needs
- Strong partnership with Amazon Web Services and currently on the Amazon MarketPlace.

Weaknesses

- Limited prime past performance at the state government level in offering Cloud Services specifically

Opportunities

- Expand footprint within state business by leveraging our current relationships built in the IT support services realms of ECM, Case Management and Records Management.
- Seek prime contracting opportunities with current customers and in our areas of expertise
- Cloud computing and IT modernization market is a fast growing area for the industry
- Corporate certifications in process (ISO 9001, CMMI Dev level 3, AWS)

Threats

- Highly competitive market
- Competitive labor market

Sales Strategies

Objectives

Growth

- Overall 5-year revenue growth – 35%
- New business – 30% of the revenue growth
- Maintain qualified BD pipeline that is continually evaluated and refreshed.
- 60% win rate
- Respond to RFIs in which we have strong qualifications and market toward the NASPO contract vehicle.
- Identify and pursue RFPs in our key capabilities areas, with states with whom we have a relationship, and that we have a strong probability to win.
- Develop relationships with additional states and their agencies through onsite visits, vendor outreach events and consistent contact management

Customer Development

- Develop a call plan for clients that revolves around their needs and the market
- Initial key states are Florida, New Hampshire, New York, and Virginia.
- Continually assess and adjust the plans to develop the relationship
- Build the relationship through visits, responding to RFIs and RFPs and establish a partnership orientation through providing thought leadership as the relationship progresses.

Pipeline Development

- Identify a short list of pre-RFP opportunities across key customers using a stringent qualification system
- Sources include GovWin, commercial databases, state acquisition forecasts, and personal visits with state representatives. Exercise a disciplined approach to determine each opportunity's qualitative and quantifiable value relevant to Armedia's business lines

- Classify each opportunity according to priority using a Salesforce based CRM
- Contact cognizant government and industry representatives for their perspectives on the relevant opportunities
- Conduct comprehensive competitive analysis, including competitor profiles, client's needs analysis and SWOT analysis relevant to the specific opportunity.

Action Plan for Success for NASPO ValuePoint (NVP) Cloud Solution

Action	Responsible Office
Develop growth plan	Business Development
Meet Stakeholders (internal) and educate them on NVP Cloud Solution	Management Team
Meet existing customers and educate them on NVP Cloud Solution, highlighting flexibility and ease of use of the vehicle.	Management Team
Develop Multi-year Pipeline of Qualified Opportunities	Business Development
Identify three new State agencies to target market	Business Development
Develop Industry call plan, including customer visits, tradeshows and conferences	Business Development
Market the NASPO ValuePoint Cloud Solution to state CPS's, staffers and potential using agencies	Business Development
Target state agencies with webinars and education sessions on current challenges that can be addressed through a cloud solution	Business Development

Resources Used in Developing Business

Dedicated Business Development Team	Conference attendance
Market Research Services, including Govwin, GovTribe, Bloomberg and FBO	Membership in key organizations, including Washington Technology, AFCEA and WIT
State Procurement Websites	Proposal consultants when needed
Salesforce CRM Platform	Dedicated Marketing Literature
Digital Marketing	Partnership Agreements
Branding	Vendor Outreach Sessions
Proposal Tools Update	PTAC and Agency specific Counseling Sessions

6.21 Related Value-Added Services to Cloud Solutions

8.20 Describe the valued-added services that you can provide as part of an awarded contract, e.g. consulting services pre- and post- implementation. Offerors may detail professional services in the RFP limited to assisting offering activities with initial setup, training and access to the services.

Besides providing ADF for developing custom business process automation applications and ACC to deploy these applications, Armedia also provides development support. The Purchasing Entity has the option to use Armedia's experienced development team to build custom solutions for their customers using ADF and deploying it on secure ACC.

Armedia also has a team of AWS certified system engineers and developers that can work with the Purchasing Entity to help their customers with cloud adoption and cloud migration.

Armedia's advanced data analytics and machine learning division can help the Purchasing Entity develop solutions for their customers centered around data warehousing, data analysis, predictive analysis and machine learning using cloud services shown in Figure 10.

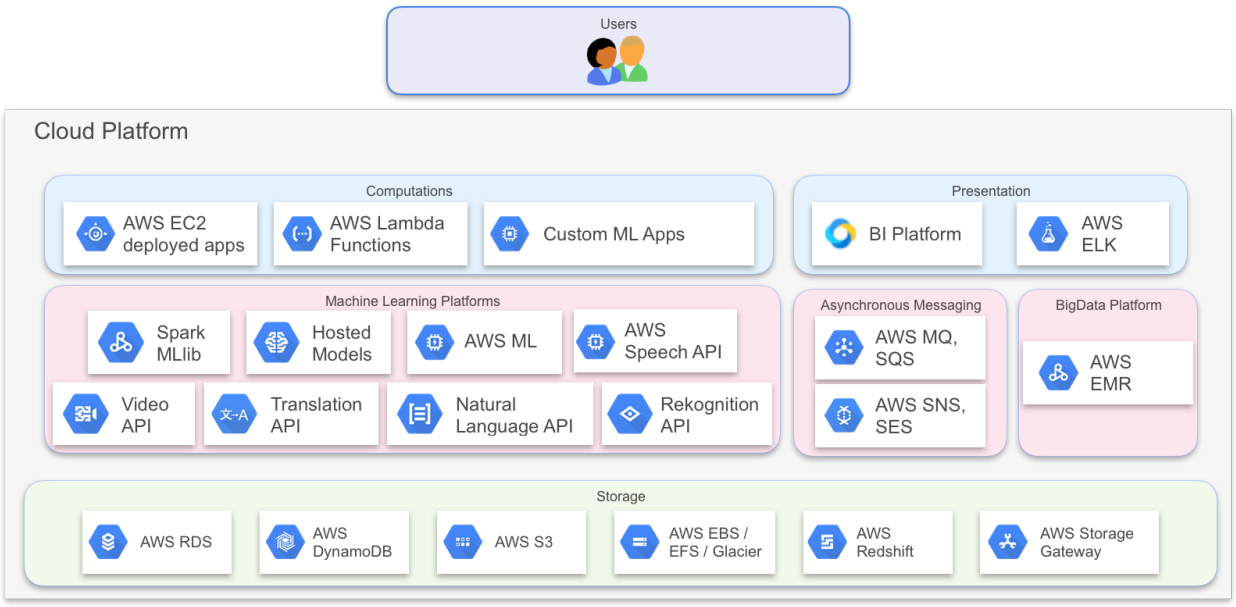


Figure 10 - Armedia's experience with cloud-based machine learning tools and solutions

6.22 Supporting Infrastructure

6.22.1 Infrastructure Needs

8.21.1 Describe what infrastructure is required by the Purchasing Entity to support your Solutions or deployment models.

ACC is designed to be auto-provisioned for ADF based solutions (Figure 7). Purchasing Entities have the option to provision additional resources and storage options based on their needs using the AWS management console.

6.22.2 Installation Needs

8.21.2 If required, who will be responsible for installation of new infrastructure and who will incur those costs?

ADF ships with support for containerized deployments using Kubernetes and Docker. The installation guide is provided along with ADF for custom installations as required.

Armedia's team of certified system engineers will work with the Purchasing Entity to help with the installation and setup of ADF based solutions when contracted.

APPENDIX A: ARKCASE VPAT

VPAT™
Voluntary Product Accessibility Template®
Version 1.3

The purpose of the **Voluntary Product Accessibility Template**, or **VPAT™**, is to assist Federal contracting officials and other buyers in making preliminary assessments regarding the availability of commercial "Electronic and Information Technology" products and services with features that support accessibility. It is assumed and recommended that offerors will provide additional contact information to facilitate more detailed inquiries.

The first table of the Template provides a summary view of the Section 508 Standards. The subsequent tables provide more detailed views of each subsection. There are three columns in each table. Column one of the Summary Table describes the subsections of subparts B and C of the Standards. The second column describes the supporting features of the product or refers you to the corresponding detailed table, e.g., "equivalent facilitation." The third column contains any additional remarks and explanations regarding the product. In the subsequent tables, the first column contains the lettered paragraphs of the subsections. The second column describes the supporting features of the product with regard to that paragraph. The third column contains any additional remarks and explanations regarding the product.

Date: 7/6/18
Name of Product: ArkCase
Contact for more Information (name/phone/email): James Bailey / (703) 272-3270 / james.bailey@armedia.com

Summary Table
VPAT™
Voluntary Product Accessibility Template®

Criteria	**Supporting Features**	**Remarks and explanations**
Section 1194.21 Software Applications and Operating Systems		
Section 1194.22 Web-based Internet Information and Applications		
Section 1194.23 Telecommunications Products		
Section 1194.24 Video and Multi-media Products		
Section 1194.25 Self-Contained, Closed Products		
Section 1194.26 Desktop and Portable Computers		

Section 1194.31 Functional Performance Criteria		
Section 1194.41 Information, Documentation and Support		

Section 1194.21 Software Applications and Operating Systems – Detail
VPAT™
Voluntary Product Accessibility Template®

Criteria	**Supporting Features**	**Remarks and explanations**
(a) When software is designed to run on a system that has a keyboard, product functions shall be executable from a keyboard where the function itself or the result of performing a function can be discerned textually.	Supported	Use of the tab key and enter keys are fully operational.
(b) Applications shall not disrupt or disable activated features of other products that are identified as accessibility features, where those features are developed and documented according to industry standards. Applications also shall not disrupt or disable activated features of any operating system that are identified as accessibility features where the application programming interface for those accessibility features has been documented by the manufacturer of the operating system and is available to the product developer.	Supported	ArkCase does not require nor does it impair any 3rd party applications. It is written on web-based standards.
(c) A well-defined on-screen indication of the current focus shall be provided that moves among interactive interface elements as the input focus changes. The focus shall be programmatically exposed so that Assistive Technology can track focus and focus changes.	Supported	We use HOVER and ACTIVE states on all of our HTML objects as well as input boxes when they are active.
(d) Sufficient information about a user interface element including the identity, operation and state of the element shall be available to Assistive Technology. When an image represents a program element,	Supported	All images are rendered using CSS with a text-equivalent in HTML.

the information conveyed by the image must also be available in text.		
(e) When bitmap images are used to identify controls, status indicators, or other programmatic elements, the meaning assigned to those images shall be consistent throughout an application's performance.	Supported	We are very consistent with our use of graphics.
(f) Textual information shall be provided through operating system functions for displaying text. The minimum information that shall be made available is text content, text input caret location, and text attributes.	Supported	The minimal information is available as text.
(g) Applications shall not override user selected contrast and color selections and other individual display attributes.	Supported	ArkCase does not override the system's contrast and display attributes.
(h) When animation is displayed, the information shall be displayable in at least one non-animated presentation mode at the option of the user.	Supported	The only animations we use are for a "loading" indication. The ALT tag on that image is "Loading. Please wait for the results to load."
(i) Color coding shall not be used as the only means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.	Supported	We use color, the use of STRONG and EM tags, and the use of H1-H6 tags to indicate information. We also use the LABEL attribute to indicate a form field title.
(j) When a product permits a user to adjust color and contrast settings, a variety of color selections capable of producing a range of contrast levels shall be provided.	N/A	Our product does not allow the user to adjust the color or contrast settings.
(k) Software shall not use flashing or blinking text, objects, or other elements having a flash or blink frequency greater than 2 Hz and lower than 55 Hz.	N/A	We do not use flashing or blinking text.
(l) When electronic forms are used, the form shall allow people using Assistive Technology to access the information, field elements, and functionality required for completion and submission of the form, including all directions and cues.	Supported	Our electronic forms support assistive technology in all of these ways.

Section 1194.22 Web-based Internet information and applications – Detail
VPAT™
Voluntary Product Accessibility Template®

Criteria	**Supporting Features**	**Remarks and explanations**
(a) A text equivalent for every non-text element shall be provided (e.g., via "alt", "longdesc", or in element content).	Supported	We do provide text equivalents everywhere.
(b) Equivalent alternatives for any multimedia presentation shall be synchronized with the presentation.	Supported	We do provide text equivalents for media, but a user must enable the accessibility setting if they choose to add a document as a PDF.
(c) Web pages shall be designed so that all information conveyed with color is also available without color, for example from context or markup.	Supported	We use emphasis tags such as STRONG and EM as well as color to convey information.
(d) Documents shall be organized so they are readable without requiring an associated style sheet.	Supported	The application is readable, although not very user friendly, without the user of a style sheet.
(e) Redundant text links shall be provided for each active region of a server-side image map.	Supported	We do not use image maps.
(f) Client-side image maps shall be provided instead of server-side image maps except where the regions cannot be defined with an available geometric shape.	Supported	We do not use image maps.
(g) Row and column headers shall be identified for data tables.	Supported	We do use table headers, footers, and caption tags to describe the tables appropriately.
(h) Markup shall be used to associate data cells and header cells for data tables that have two or more logical levels of row or column headers.	Supported	We do associate our cells with our headers for easy tabbing using assistive technology.
(i) Frames shall be titled with text that facilitates frame identification and navigation	Supported	We do not use frames.

(j) Pages shall be designed to avoid causing the screen to flicker with a frequency greater than 2 Hz and lower than 55 Hz.	Supported	We do not use a flicker or animation.
(k) A text-only page, with equivalent information or functionality, shall be provided to make a web site comply with the provisions of this part, when compliance cannot be accomplished in any other way. The content of the text-only page shall be updated whenever the primary page changes.	Not Applicable	We do not provide a text-only version of the application because our product is already accessible.
(l) When pages utilize scripting languages to display content, or to create interface elements, the information provided by the script shall be identified with functional text that can be read by Assistive Technology.	Supported	We do our best to let the user know when content been changed and assistive technology will help the user do that.
(m) When a web page requires that an applet, plug-in or other application be present on the client system to interpret page content, the page must provide a link to a plug-in or applet that complies with §1194.21(a) through (l).	Supported	When 3rd party plugins are used, we provide a link to the plug-in for the user to download.
(n) When electronic forms are designed to be completed on-line, the form shall allow people using Assistive Technology to access the information, field elements, and functionality required for completion and submission of the form, including all directions and cues.	Supported	We do support this.
(o) A method shall be provided that permits users to skip repetitive navigation links.	Supported	We support this.
(p) When a timed response is required, the user shall be alerted and given sufficient time to indicate more time is required.	Supported	We do have a timeout that the user is alerted to and they'r egiven the option to extend their session.

Note to 1194.22: The Board interprets paragraphs (a) through (k) of this section as consistent with the following priority 1 Checkpoints of the Web Content Accessibility Guidelines 1.0 (WCAG 1.0) (May 5 1999) published by the Web Accessibility Initiative of the World Wide Web Consortium: Paragraph (a) - 1.1, (b) - 1.4, (c) - 2.1, (d) - 6.1, (e) - 1.2, (f) - 9.1, (g) - 5.1, (h) - 5.2, (i) - 12.1, (j) - 7.1, (k) - 11.4.

Section 1194.23 Telecommunications Products – Detail
VPAT™
Voluntary Product Accessibility Template®

Criteria	**Supporting Features**	**Remarks and explanations**
(a) Telecommunications products or systems which provide a function allowing voice communication and which do not themselves provide a TTY functionality shall provide a standard non-acoustic connection point for TTYs. Microphones shall be capable of being turned on and off to allow the user to intermix speech with TTY use.	N/A	
(b) Telecommunications products which include voice communication functionality shall support all commonly used cross-manufacturer non-proprietary standard TTY signal protocols.	N/A	
(c) Voice mail, auto-attendant, and interactive voice response telecommunications systems shall be usable by TTY users with their TTYs.	N/A	
(d) Voice mail, messaging, auto-attendant, and interactive voice response telecommunications systems that require a response from a user within a time interval, shall give an alert when the time interval is about to run out, and shall provide sufficient time for the user to indicate more time is required.	N/A	
(e) Where provided, caller identification and similar telecommunications functions shall also be available for users of TTYs, and for users who cannot see displays.	N/A	
(f) For transmitted voice signals, telecommunications products shall provide a gain adjustable up to a minimum of 20 dB. For incremental volume control, at least one intermediate step of 12 dB of gain shall be provided.	N/A	
(g) If the telecommunications product allows a user to adjust the receive	N/A	

volume, a function shall be provided to automatically reset the volume to the default level after every use.		
(h) Where a telecommunications product delivers output by an audio transducer which is normally held up to the ear, a means for effective magnetic wireless coupling to hearing technologies shall be provided.	N/A	
(i) Interference to hearing technologies (including hearing aids, cochlear implants, and assistive listening devices) shall be reduced to the lowest possible level that allows a user of hearing technologies to utilize the telecommunications product.	N/A	
(j) Products that transmit or conduct information or communication, shall pass through cross-manufacturer, non-proprietary, industry-standard codes, translation protocols, formats or other information necessary to provide the information or communication in a usable format. Technologies which use encoding, signal compression, format transformation, or similar techniques shall not remove information needed for access or shall restore it upon delivery.	N/A	
(k)(1) Products which have mechanically operated controls or keys shall comply with the following: Controls and Keys shall be tactilely discernible without activating the controls or keys.	N/A	
(k)(2) Products which have mechanically operated controls or keys shall comply with the following: Controls and Keys shall be operable with one hand and shall not require tight grasping, pinching, twisting of the wrist. The force required to activate controls and keys shall be 5 lbs. (22.2N) maximum.	N/A	
(k)(3) Products which have mechanically operated controls or keys shall comply with the following: If key repeat is supported, the delay before repeat shall be adjustable to at least 2 seconds. Key	N/A	

repeat rate shall be adjustable to 2 seconds per character.		
(k)(4) Products which have mechanically operated controls or keys shall comply with the following: The status of all locking or toggle controls or keys shall be visually discernible, and discernible either through touch or sound.	N/A	

Section 1194.24 Video and Multi-media Products – Detail
VPAT™
Voluntary Product Accessibility Template®

Criteria	**Supporting Features**	**Remarks and explanations**
a) All analog television displays 13 inches and larger, and computer equipment that includes analog television receiver or display circuitry, shall be equipped with caption decoder circuitry which appropriately receives, decodes, and displays closed captions from broadcast, cable, videotape, and DVD signals. As soon as practicable, but not later than July 1, 2002, widescreen digital television (DTV) displays measuring at least 7.8 inches vertically, DTV sets with conventional displays measuring at least 13 inches vertically, and stand-alone DTV tuners, whether or not they are marketed with display screens, and computer equipment that includes DTV receiver or display circuitry, shall be equipped with caption decoder circuitry which appropriately receives, decodes, and displays closed captions from broadcast, cable, videotape, and DVD signals.	N/A	
(b) Television tuners, including tuner cards for use in computers, shall be equipped with secondary audio program playback circuitry.	N/A	
(c) All training and informational video and multimedia productions which support the agency's mission, regardless of format, that contain speech or other audio information	N/A	

necessary for the comprehension of the content, shall be open or closed captioned.		
(d) All training and informational video and multimedia productions which support the agency's mission, regardless of format, that contain visual information necessary for the comprehension of the content, shall be audio described.	N/A	
(e) Display or presentation of alternate text presentation or audio descriptions shall be user-selectable unless permanent.	N/A	

Section 1194.25 Self-Contained, Closed Products – Detail
VPAT™
Voluntary Product Accessibility Template®

Criteria	**Supporting Features**	**Remarks and explanations**
(a) Self contained products shall be usable by people with disabilities without requiring an end-user to attach Assistive Technology to the product. Personal headsets for private listening are not Assistive Technology.	N/A	
(b) When a timed response is required, the user shall be alerted and given sufficient time to indicate more time is required.	N/A	
(c) Where a product utilizes touchscreens or contact-sensitive controls, an input method shall be provided that complies with §1194.23 (k) (1) through (4).	N/A	
(d) When biometric forms of user identification or control are used, an alternative form of identification or activation, which does not require the user to possess particular biological characteristics, shall also be provided.	N/A	
(e) When products provide auditory output, the audio signal shall be provided at a standard signal level through an industry standard connector that will allow for private listening. The product must provide	N/A	

the ability to interrupt, pause, and restart the audio at anytime.		
(f) When products deliver voice output in a public area, incremental volume control shall be provided with output amplification up to a level of at least 65 dB. Where the ambient noise level of the environment is above 45 dB, a volume gain of at least 20 dB above the ambient level shall be user selectable. A function shall be provided to automatically reset the volume to the default level after every use.	N/A	
(g) Color coding shall not be used as the only means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.	N/A	
(h) When a product permits a user to adjust color and contrast settings, a range of color selections capable of producing a variety of contrast levels shall be provided.	N/A	
(i) Products shall be designed to avoid causing the screen to flicker with a frequency greater than 2 Hz and lower than 55 Hz.	N/A	
(j) (1) Products which are freestanding, non-portable, and intended to be used in one location and which have operable controls shall comply with the following: The position of any operable control shall be determined with respect to a vertical plane, which is 48 inches in length, centered on the operable control, and at the maximum protrusion of the product within the 48 inch length on products which are freestanding, non-portable, and intended to be used in one location and which have operable controls.	N/A	
(j)(2) Products which are freestanding, non-portable, and intended to be used in one location and which have operable controls shall comply with the following: Where any operable control is 10 inches or less behind the reference plane, the height shall be 54 inches maximum and 15 inches minimum above the floor.	N/A	

(j)(3) Products which are freestanding, non-portable, and intended to be used in one location and which have operable controls shall comply with the following: Where any operable control is more than 10 inches and not more than 24 inches behind the reference plane, the height shall be 46 inches maximum and 15 inches minimum above the floor.	N/A	
(j)(4) Products which are freestanding, non-portable, and intended to be used in one location and which have operable controls shall comply with the following: Operable controls shall not be more than 24 inches behind the reference plane.	N/A	

Section 1194.26 Desktop and Portable Computers – Detail
VPAT™
Voluntary Product Accessibility Template®

Criteria	**Supporting Features**	**Remarks and explanations**
(a) All mechanically operated controls and keys shall comply with §1194.23 (k) (1) through (4).	N/A	
(b) If a product utilizes touchscreens or touch-operated controls, an input method shall be provided that complies with §1194.23 (k) (1) through (4).	N/A	
(c) When biometric forms of user identification or control are used, an alternative form of identification or activation, which does not require the user to possess particular biological characteristics, shall also be provided.	N/A	
(d) Where provided, at least one of each type of expansion slots, ports and connectors shall comply with publicly available industry standards	N/A	

Section 1194.31 Functional Performance Criteria – Detail
VPAT™

Voluntary Product Accessibility Template®

Criteria	**Supporting Features**	**Remarks and explanations**
(a) At least one mode of operation and information retrieval that does not require user vision shall be provided, or support for Assistive Technology used by people who are blind or visually impaired shall be provided.	N/A	
(b) At least one mode of operation and information retrieval that does not require visual acuity greater than 20/70 shall be provided in audio and enlarged print output working together or independently, or support for Assistive Technology used by people who are visually impaired shall be provided.	N/A	
(c) At least one mode of operation and information retrieval that does not require user hearing shall be provided, or support for Assistive Technology used by people who are deaf or hard of hearing shall be provided	N/A	
(d) Where audio information is important for the use of a product, at least one mode of operation and information retrieval shall be provided in an enhanced auditory fashion, or support for assistive hearing devices shall be provided.	N/A	
(e) At least one mode of operation and information retrieval that does not require user speech shall be provided, or support for Assistive Technology used by people with disabilities shall be provided.	N/A	
(f) At least one mode of operation and information retrieval that does not require fine motor control or simultaneous actions and that is operable with limited reach and strength shall be provided.	N/A	

Section 1194.41 Information, Documentation and Support – Detail
VPAT™

Voluntary Product Accessibility Template®		
Criteria	**Supporting Features**	**Remarks and explanations**
(a) Product support documentation provided to end-users shall be made available in alternate formats upon request, at no additional charge	Not Supported	Needs further investigation.
(b) End-users shall have access to a description of the accessibility and compatibility features of products in alternate formats or alternate methods upon request, at no additional charge.	Not Supported	Needs further investigation.
(c) Support services for products shall accommodate the communication needs of end-users with disabilities.	Not Supported	Needs further investigation.

APPENDIX B: ALFRESCO VPAT

Voluntary Product Accessibility Template

Version 1.8

Date: February 01, 2017
Name of Product: Alfresco Share 5.2
Contact for more Information: John.Knowles@Alfresco.com

Product description:

Alfresco Share provides content management capabilities with simple user interfaces, tools to search and browse the repository, content such as thumbnails and associated metadata and a set of collaboration tools such as Wikis, Discussions, and Blogs. Alfresco Share is organized as a set of sites that can be used as a meeting place for collaboration.

Summary Table – Voluntary Product Accessibility Template

Criteria	Supporting Features	Remarks and Explanations
Section 1194.21 Software Applications and Operating Systems	Not Applicable	
Section 1194.22 Web-based internet information and applications	Included	Web-based product
Section 1194.23 Telecommunications Products	Not Applicable	
Section 1194.24 Video and Multi-media Products	Not Applicable	
Section 1194.25 Self-Contained, Closed Products	Not Applicable	
Section 1194.26 Desktop and Portable Computers	Not Applicable	
Section 1194.31 Functional Performance Criteria	Included	
Section 1194.41 Information, Documentation and Support - Detail	Included	

Section 1194.22 Web-based Internet information and applications – Detail – Voluntary Product Accessibility Template

Criteria	Supporting Features	Remarks and Explanations
(a) A text equivalent for every non-text element shall be provided (e.g., via "alt", "longdesc", or in element content).	Supported with Exceptions	The majority of instances for non-text have alternative text provided.
(b) Equivalent alternatives for any multimedia presentation shall be synchronized with the presentation.	Supported	For some document types, Alfresco provides a document preview using HTML5. The original document is available as an equivalent alternative. This is an optional feature and not required for successful use of the application.
(c) Web pages shall be designed so that all information conveyed with color is also available without color, for example from context or markup.	Supported	Where color-coding is used, it is not a primary method of conveying information.
(d) Documents shall be organized so they are readable without requiring an associated style sheet.	Supported with Exceptions	Equivalent Facilitation is provided to support low vision users in high contrast. A high contrast theme is provided as standard with the product. In order to view the application logically, styles that define element layout cannot be ignored
(e) Redundant text links shall be provided for each active region of a server-side image map.	Not Applicable	The application does not use server-side image maps.
(f) Client-side image maps shall be provided instead of server-side image maps except where the regions cannot be defined with an available geometric shape.	Not Applicable	The application does not use server-side image maps.
(g) Row and column headers shall be identified for data tables.	Supported with Exceptions	Some tables do not include column headers.
(h) Markup shall be used to associate data cells and header cells for data tables that have two or more logical levels of row or column headers.	Supported with Exceptions	Some tables do not include column headers.
(i) Frames shall be titled with text that facilitates frame identification and navigation.	Supported	

Criteria	Supporting Features	Remarks and Explanations
(j) Pages shall be designed to avoid causing the screen to flicker with a frequency greater than 2 Hz and lower than 55 Hz.	Supported	The application does not use blinking or flickering content.
(k) A text-only page, with equivalent information or functionality, shall be provided to make a web site comply with the provisions of this part, when compliance cannot be accomplished in any other way. The content of the text-only page shall be updated whenever the primary page changes.	Not Applicable	Modern technologies provide for non-textual views of the content available in the browser.
(l) When pages utilize scripting languages to display content, or to create interface elements, the information provided by the script shall be identified with functional text that can be read by Assistive Technology.	Supported with Exceptions	Most scripted areas of the application provide text that can be used by assistive technologies. Some areas of the application (such as hierarchical-tree based navigation) provide support via equivalent facilitation such as breadcrumb style navigation.
(m) When a web page requires that an applet, plug-in or other application be present on the client system to interpret page content, the page must provide a link to a plug-in or applet that complies with §1194.21(a) through (l).	Supported	There are no mandatory applets, plugins, or similar required. HTML5 is optionally used for document previews and uploads.
(n) When electronic forms are designed to be completed on-line, the form shall allow people using Assistive Technology to access the information, field elements, and functionality required for completion and submission of the form, including all directions and cues.	Supported with Exceptions	Forms may be keyboard driven. A small number of editable fields and/or controls not have labels associated with them.
(o) A method shall be provided that permits users to skip repetitive navigation links.	Supported with Exceptions	Currently, the application provides skip navigation links or methods, for example in the common header and in search pages. Some pages are not currently fully supported
(p) When a timed response is required, the user shall be alerted and	Not Applicable	Alfresco Share does not require a timed response as

Criteria	Supporting Features	Remarks and Explanations
given sufficient time to indicate more time is required.		part of its core functionality.

Section–1194.31 Functional Performance Criteria – Detail – Voluntary Product Accessibility Template

Criteria	Supporting Features	Remarks and Explanations
(a) At least one mode of operation and information retrieval that does not require user vision shall be provided, or support for Assistive Technology used by people who are blind or visually impaired shall be provided.	Supported	Assistive Technologies compatible with the operating systems and Web browsers supported by Alfresco can be used.
(b) At least one mode of operation and information retrieval that does not require visual acuity greater than 20/70 shall be provided in audio and enlarged print output working together or independently, or support for Assistive Technology used by people who are visually impaired shall be provided.	Supported	Assistive Technologies compatible with the operating systems and Web browsers supported by Alfresco can be used.
(c) At least one mode of operation and information retrieval that does not require user hearing shall be provided, or support for Assistive Technology used by people who are deaf or hard of hearing shall be provided	Not Applicable	Alfresco Share does not require user hearing.
(d) Where audio information is important for the use of a product, at least one mode of operation and information retrieval shall be provided in an enhanced auditory fashion, or support for assistive hearing devices shall be provided.	Not Applicable	Alfresco Share does not require user hearing.
(e) At least one mode of operation and information retrieval that does not require user speech shall be provided, or support for Assistive Technology used by people with disabilities shall be provided.	Not Applicable	Alfresco Share does not require user hearing.
(f) At least one mode of operation and information retrieval that does not require fine motor control or	Supported	Assistive Technologies compatible with the operating systems and Web

Criteria	Supporting Features	Remarks and Explanations
simultaneous actions and that is operable with limited reach and strength shall be provided.		browsers supported by Alfresco Share can be used.

Section–1194.41 Information, Documentation and Support – Detail – Voluntary Product Accessibility Template

Criteria	Supporting Features	Remarks and Explanations
(a) Product support documentation provided to end-users shall be made available in alternate formats upon request, at no additional charge	Supported	Alfresco provides electronic versions of all product support documentation
(b) End-users shall have access to a description of the accessibility and compatibility features of products in alternate formats or alternate methods upon request, at no additional charge.	Supported	Requests should be made through Alfresco Customer Support. See www.alfresco.com for details.
(c) Support services for products shall accommodate the communication needs of end-users with disabilities.	Supported	Product support for Alfresco Share is available in a variety of formats and from a number of online sources available from Alfresco Software, Inc.

This document is for informational purposes only.
ALFRESCO MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

ARKCASE END USER LICENSE AGREEMENT

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE PURCHASING AND/OR USING SOFTWARE OR SUPPORT FROM ARKCASE. BY USING ARKCASE SOFTWARE OR SUPPORT, USER ACCEPTS THIS AGREEMENT AND ACKNOWLEDGES IT HAS READ AND UNDERSTANDS THIS AGREEMENT. AN INDIVIDUAL ACTING ON BEHALF OF AN ENTITY REPRESENTS THAT HE OR SHE HAS THE AUTHORITY TO ENTER INTO THIS AGREEMENT ON BEHALF OF THAT ENTITY. IF USER DOES NOT ACCEPT THE TERMS OF THIS AGREEMENT, THEN IT MUST NOT USE ARKCASE SOFTWARE OR SUPPORT.

This ArkCase End User License Agreement (the "Agreement") is between ArkCase, LLC, a Virginia, LLC (“ArkCase”), and the individual or entity that accepts the terms of this Agreement ("User"). The effective date of this Agreement (“Effective Date”) is the earlier of the date that User formally accepts this Agreement or first uses ArkCase’s Software or Support.

1. SCOPE OF AGREEMENT

1.1 Software and Support. This Agreement governs User’s use of ArkCase Software and, if applicable, Support. “Support” means ArkCase maintenance and support. "Software" means the software accompanying this Agreement and branded by ArkCase; provided, Software does not include third-party open source software that may be provided therewith or Community Versions. “Community Versions” means the free, unsupported, open-source software that ArkCase may make available for download on its ArkCase web site. “Order Form” means the ordering documents placed by User. "Subscription" means access to the Software and, where applicable, Support for a defined period of time (the “Subscription Period”), as set forth in an Order Form.

1.2. Business Partners. User is purchasing Software and Support from an ArkCase business partner (a "Business Partner"). ArkCase will provide the purchased Software and Support to User under the terms of this Agreement, but is not responsible for (a) the actions of Business Partners, (b) any additional obligations Business Partners may have to User, or (c) any non-ArkCase products or services that Business Partners supply to User.

2. REPORTING AND RECORDS

2.1 Reporting. User will notify ArkCase or the Business Partner promptly if User exceeds the number authorized CPUs purchased under the applicable Order Form. In its notice, User will include the number of CPUs, and the date User exceeded its licensed CPUs. ArkCase (or the Business Partner) will invoice User for the applicable fees and User will promptly pay such fees.

2.2 Records Retention. User will maintain accurate records necessary to verify the number of CPUs it authorizes. Upon ArkCase's written request, User will provide ArkCase such records within ten (10) business days.

3. LICENSE AND OWNERSHIP

3.1 Grant to User. Subject to User's compliance with this Agreement, ArkCase grants to User, during the Subscription Period: (a) a non-exclusive, non-transferable, non-sublicensable license to use, copy, test, and modify the Software solely for User's own internal use and limited to the number of CPUs, Cores, Named Users, and/or Active Processes designated in the Order Form, as applicable; (b) the rights in the third party open-source software provided with the Software, which rights are set forth in the applicable third-party licenses; and (c) for the term designated in an Order Form, the right to receive Support. A “Central Processing Unit (CPU)” is the electronic circuitry within a computer that carries out the instructions of a computer program by performing the basic arithmetic, logical, control and input/output (I/O) operations specified by the instructions. A “Core” is usually the basic computation unit of the CPU. A “Named User” is an individual authorized by User to access the Software and who has been given a unique user name or identifier (regardless of whether the user has actually used those credentials to access the Software). No more than one individual may use an issued user name or identifier, and the sharing of such credentials is expressly prohibited. “Active Process,” as used with purchases of ArkCase Activiti BPM software, means a process instance within the Software that has not been completed, cancelled, or formally suspended. Processes that have been initiated—but which have not been completed, cancelled, or formally

suspended, or which are in a "wait" state— shall constitute Active Processes regardless of the level of user or machine activity associated with those processes over time.

3.2 Restrictions. User will not, directly or indirectly: (a) sublicense, resell, rent, lease, distribute, market, commercialize or otherwise transfer rights or usage to: (i) the Software, (ii) any modified version or derivative work of the Software created by the User or for the User, or (iii) Community Versions; (b) remove or alter any copyright, trademark or proprietary notice in the Software; (c) transfer, use or export the Software in violation of any laws or regulations of any government; or (e) reverse engineer, decompile or modify any encrypted or encoded portion of the Software.

3.3 Proprietary Rights. ArkCase and its licensors will own all right, title, and interest to the Software, Support, technology, information, code or software provided to User by ArkCase, including all copies or modifications made by ArkCase.

4. TERM AND TERMINATION

4.1 Term and Termination of Agreement. This Agreement will remain in effect for the duration of any active Subscription Period. Upon termination of User's Subscription Period, User will not have access to support, upgrades, patches, enhancements, or any improvements of ArkCase. If User materially breaches the terms of this Agreement, and the breach is not cured (or curable) within thirty (30) days after written notice of the breach, then ArkCase may, upon written notice, to the breaching party, terminate this Agreement and User's access to the Software and Support.

4.2 Survival. If this Agreement is terminated for any reason, Sections 3.2, 3.3, 4.1, 4.2, 5, 6.2, 7, 8 and 9 of this Agreement will survive termination.

5. CONFIDENTIALITY

5.1 Confidential Information.

(a) Definition. In connection with this Agreement, either party (the "Recipient") may obtain confidential and proprietary information ("Confidential Information") from the other (the "Discloser"). Confidential Information may include, without limitation, information about systems designs, pricing, cost data, financial information, business, sales, and marketing plans, products, product roadmaps, service programs, trade secrets, know-how, inventions, techniques, processes, programs, schematics, software, and data. Confidential Information includes information designated in writing as confidential, and any information a reasonable person would understand to be confidential or proprietary under the circumstances of its disclosure.

(b) Exclusions. "Confidential Information" does not include information that: (i) has been independently developed by or for the Recipient without access or reference to, or use of, Confidential Information; (ii) is lawfully received free of restriction from another source having the right to furnish such information; (iii) is or becomes lawfully in the public domain other than through a breach of this Agreement; (iv) was lawfully known by the Recipient prior to disclosure; (v) Discloser agrees in writing is free of such restrictions; or (vi) is generally disclosed by the Discloser to third parties without a duty of confidentiality.

(c) Duties With Respect To Confidential Information. At all times during and after the term of this Agreement, Recipient shall keep Discloser's Confidential Information confidential using the same degree of care that it uses to protect its own Confidential Information, but not less than a reasonable degree of care, and shall not disclose Discloser's Confidential Information to a third party without the Discloser's written consent, or use the Confidential Information for purposes other than the performance of this Agreement. Where disclosure is required by law, such disclosure shall not constitute a breach of this Agreement provided Recipient gives Discloser reasonable advance notice to enable Discloser to seek appropriate protection of the Confidential Information.

6. REPRESENTATIONS AND WARRANTIES

6.1 General Representations and Warranties. ArkCase represents and warrants that: (a) it will use reasonable skill and care in providing contracted Support; (b) the Support will be performed in a professional and workmanlike manner by qualified

personnel; (c) it has the authority to enter into this Agreement with User; and (d) ArkCase has taken commercially reasonable measures to ensure the Software does not, at the time of delivery to User, include malicious mechanisms or code designed to damage or corrupt the Software.

6.2 Disclaimer of Warranty. EXCEPT AS EXPRESSLY PROVIDED IN SECTION 6.1, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE SOFTWARE AND SUPPORT PROVIDED BY ARKCASE ARE PROVIDED WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE. ARKCASE DOES NOT GUARANTEE THAT THE USE OF THE SOFTWARE OR SUPPORT WILL BE UNINTERRUPTED, ERROR FREE, OR THAT ARKCASE WILL CORRECT ALL SOFTWARE ERRORS. FOR THE BREACH OF THE WARRANTIES SET FORTH IN SECTION 6.1, USER'S EXCLUSIVE REMEDY AND ARKCASE'S ENTIRE LIABILITY WILL BE TO UNDERTAKE COMMERCIALLY REASONABLE EFFORTS TO REMEDY THE SUPPORT DEFICIENCY, SUPPLY A TEMPORARY FIX, OR MAKE AN EMERGENCY BYPASS. IF ARKCASE CANNOT SUBSTANTIALLY CORRECT A BREACH IN A COMMERCIALLY REASONABLE MANNER, USER MAY TERMINATE THE RELEVANT SOFTWARE SUBSCRIPTION AND RECEIVE A PRO RATA REFUND OF FEES PAID FOR THE REMAINING SUBSCRIPTION PERIOD AS OF THE EFFECTIVE DATE OF THE TERMINATION.

7. LIMITATION OF LIABILITY AND DISCLAIMER OF DAMAGES

7.1 Disclaimer of Damages. NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS AGREEMENT OR AN ORDER FORM, IN NO EVENT WILL EITHER PARTY OR ITS AFFILIATES BE LIABLE TO THE OTHER PARTY OR ITS AFFILIATES FOR DAMAGES OTHER THAN DIRECT DAMAGES, INCLUDING, WITHOUT LIMITATION: ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY OR PUNITIVE DAMAGES, WHETHER IN TORT, (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE; OR ANY DAMAGES ARISING OUT OF OR IN CONNECTION WITH ANY MALFUNCTIONS, REGULATORY NONCOMPLIANCE, DELAYS, LOSS OF DATA, LOST PROFITS, LOST SAVINGS, INTERRUPTION OF SERVICE, LOSS OF BUSINESS OR ANTICIPATORY PROFITS, EVEN A PARTY OR ITS AFFILIATES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. LIABILITY FOR THESE DAMAGES WILL BE LIMITED AND EXCLUDED EVEN IF ANY EXCLUSIVE REMEDY PROVIDED FOR IN THIS AGREEMENT FAILS OF ITS ESSENTIAL PURPOSE.

7.2 Limitation of Liability. NEITHER PARTY'S (OR ITS AFFILIATES') AGGREGATE AND CUMULATIVE LIABILITY ARISING FROM OR RELATING TO THIS AGREEMENT, WHETHER IN CONTRACT, TORT, STATUTE OR OTHERWISE WILL EXCEED THE AMOUNTS PAID OR OWED TO ARKCASE BY USER, EITHER DIRECTLY OR THROUGH A BUSINESS PARTNER, DURING THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE FIRST EVENT GIVING RISE TO LIABILITY. NOTHING IN THIS AGREEMENT IS INTENDED TO EXCLUDE OR LIMIT EITHER PARTY'S LIABILITY FOR DEATH, PERSONAL INJURY, OR PROPERTY DAMAGE CAUSED BY NEGLIGENCE, OR FOR FRAUD. NOTHING IN THIS SECTION WILL LIMIT THE FEES OWED BY USER UNDER THIS AGREEMENT FOR SOFTWARE OR SUPPORT, OR FOR EXCEEDING THE SCOPE OF THE LICENSES GRANTED OR VIOLATING THE RESTRICTIONS IN SECTION 3.

8. INDEMNIFICATION

8.1 Defense. If a third party initiates or threatens a legal action alleging that User's use of the Software directly infringes the third party's patent, copyright, trademark or misappropriates the third party's trade secret rights ("Third Party Rights") (such action, a "Claim"), then ArkCase will (a) promptly assume the defense of the Claim and (b) pay costs, damages and/or reasonable attorneys' fees that are included in a final judgment against User (without right of appeal) or in a settlement approved by ArkCase that are attributable to User's use of the Software; provided that User (i) is current in the payment of all applicable fees, or becomes current, prior to requesting indemnification, (ii) notifies ArkCase in writing of the Claim promptly after receipt of the Claim, (iii) provides ArkCase the right to control the defense of the Claim with counsel of its choice, and to settle such Claim at ArkCase's sole discretion (unless the settlement requires payment by User or requires User to admit liability), and (iv) reasonably cooperates with ArkCase in the defense of the Claim.

8.2 Injunctive Relief. If the Software becomes the subject of any actual or anticipated third party infringement claim, ArkCase may, at its sole option and expense, (i) procure for User the right to continue using the affected Software consistent with this Agreement, (ii) replace or modify the affected Software with functionally equivalent software that does not infringe, or, if either (i) or (ii) is not available on a basis that ArkCase finds commercially feasible, (iii) terminate the Agreement or applicable Order Form and refund any prepaid fees for all unused portions of the Subscription Period.

8.3 Exclusions. ArkCase will have no liability for any Claim based upon (a) use of non-current versions of the Software when ArkCase has made newer, non-infringing versions available User; (b) altered versions of the Software (unless the specific alteration was made by or for ArkCase); (c) use, operation or combination of the applicable Software with non-ArkCase programs, data, equipment or documentation if such infringement would have been avoided but for such use, operation or combination; (d) ArkCase's compliance with designs, specifications or instructions provided by User where those designs, specifications or instructions cause the infringement; (e) use by User after notice by ArkCase to discontinue use of all or a portion of the Software; or (f) third-party open-source software. This section constitutes the entire liability of ArkCase, and User's sole and exclusive remedy, with respect to any third party claims of infringement or misappropriation of intellectual property rights.

9. GENERAL

9.1 Notices. Notices under this Agreement must be in writing and delivered: (a) if to ArkCase, to its Chief Financial Officer, with a copy to its General Counsel; (b) if to User, to its Chief Financial Officer or any individual identified in the Order Form. Notices will be deemed received when (1) delivered personally; or (2) upon confirmed delivery by a commercial express carrier.

9.2 Compliance with Applicable Laws. Each party will comply with all applicable laws, including applicable export control restrictions. In order for ArkCase to provide Support to User, it may be necessary for ArkCase to share information with its Affiliates, Business Partners, and/or subcontractors, which may be located worldwide. In such event, ArkCase will comply with Section 5 of this Agreement and with applicable data privacy laws governing the transfer of that information. This Agreement will be interpreted and construed in accordance with the laws of the District of Columbia and the United States of America, excluding that body of law applicable to choice of law. The parties agree that in the event a lawsuit is filed by User, the parties consent to jurisdiction in the state or federal courts for the District of Columbia and, in the event a lawsuit is filed by ArkCase, the parties consent to jurisdiction in the state or federal courts of the District of Columbia, and in each such case such venue shall not be challenged by the non-filing party as improper or inappropriate due to, among other things, inconvenience under the doctrine of forum non-convenience or other similar doctrines. Each party also agrees not to bring any action or proceeding arising out of or relating to this Agreement in any other court.

9.3 Entire Agreement. Except as otherwise provided in a signed agreement between the parties, this Agreement constitutes the exclusive and complete agreement between ArkCase and User with respect to User's use of ArkCase Software and/or Support, and supersedes all prior oral or written discussions, agreements or understandings.

9.4 Force Majeure. Force majeure events shall excuse the affected party (the "Non-Performing Party") from its obligations under this Agreement so long as the event and its effects continue. Force majeure events include, without limitation, Acts of God, natural disasters, war, riot, network attacks, acts of terrorism, fire, explosion, accident, sabotage, strikes, inability to obtain power, fuel, material or labor, or acts of any government. As soon as feasible, the Non-Performing Party shall notify the other party of (a) its best reasonable assessment of the nature and duration of the force majeure event, and (b) the steps it is taking to mitigate its effects. If the force majeure event prevents performance for more than sixty (60) consecutive days, and the parties have not agreed upon a revised basis for performance, then either party may immediately terminate the Agreement upon written notice.

9.5 Severability/Waiver. If any provision of this Agreement is ruled invalid or unenforceable, the provision shall be severable from this Agreement so that the remaining provisions are unaffected. No waiver of any rights under this Agreement will constitute a subsequent waiver unless otherwise stated in writing.

9.6 Dispute Resolution. English law shall govern all aspects of this Agreement. Any dispute arising from this Agreement shall be subject to the exclusive jurisdiction of courts located in England and Wales, without regard to their conflict-of-law principles or the United Nations Convention on Contracts for the International Sale of Goods.

9.7 Headings. All headings contained in this Agreement are inserted for identification and convenience and will not be deemed part of this Agreement for purposes of interpretation.

9.8 Amendment. This Agreement may not be amended or modified except in a writing signed by the parties, with specific reference to this Agreement.

9.9 Export Controls. User acknowledges that ArkCase makes no representation or warranty that the ArkCase Products may be exported without appropriate licenses or permits under applicable law, or that any such license or permit has been, will be or can be obtained. User will comply with all applicable export and import control laws and regulations in its use of the ArkCase Products. User will not, directly or indirectly, export or re-export, or knowingly permit the export or re-export of any ArkCase Products to any country for which approval is required under the laws of the United States or any other country unless the appropriate export license or approval has first been obtained. User confirms that it will not export or re-export the ArkCase Products, directly or indirectly, to (i) any countries that are subject to United States export restrictions (at the execution of this contract such countries include Cuba, Iran, Libya, North Korea, Sudan and Syria); or (ii) to any End User whom User knows or has reason to know will utilize them in the design, development or production of nuclear, chemical or biological weapons. In addition, if ArkCase informs User that, or User knows or has reason to know that, any ArkCase Product contains encryption or other capabilities subject to the International Traffic in Arms Regulations (ITAR) set forth at 22 C.F.R. section 120 et seq., User shall not export such Product in violation of ITAR.

9.10 U.S. Government End-Users. Each of the components that constitute the ArkCase Software is a “commercial item” as that term is defined at 48 C.F.R. 2.101, consisting of “commercial computer software” and/or “commercial computer software documentation” as such terms are used in 48 C.F.R. 12.212. Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4, all U.S. Government end users acquire the ArkCase Software with only those rights set forth herein.

THE FOLLOWING APPLIES ONLY IF USER HAS PURCHASED DIRECT ARKCASE SUPPORT

Attachment 1

(ArkCase Support)

1. ArkCase Support Programs. ArkCase's support offerings, service levels, and guidelines are set forth at http://www.arkcase.com/docs. If User has purchased support, User's applicable support program(s) will be set forth in the Order Form. ArkCase support may be used only for User's internal purposes. Use of ArkCase support on behalf of a third party that is not a party to the Agreement, or for Community Versions, is a material breach of the Agreement.

2.1 Scope of Support. In using ArkCase support, User agrees it will: (a) provide ArkCase with sufficient information and resources to correct the applicable support issue; (b) install and operate the Software on an ArkCase-supported stack, as identified at http://www.arkcase.com/docs; (c) promptly install all service packs provided by ArkCase; and (d) procure, install and maintain all equipment, telephone lines, communication interfaces and other hardware necessary to operate the Software.

User is responsible for reading the release notes and any other available documentation before installing or upgrading the Software, and for testing the Software before deploying it in a production environment. User should also backup its production systems on a regular basis and have those backups available if needed for support purposes. ArkCase is not obligated to provide for the following: (a) Software that has been modified or damaged by customer or a third party (unless at ArkCase's direction); (b) issues caused by User's negligence, hardware malfunction or other causes beyond the reasonable control of ArkCase; (c) issues caused by third party software not licensed through ArkCase or provided by ArkCase.

2.2 Technical Support Contacts. ArkCase customer support will provide Support to the designated contacts, as identified in an Order Form ("Technical Support Contacts"). The Technical Support Contacts should have "read, write and execute" access to the necessary files, English language communication skills and relevant technical knowledge. User may modify its designated Technical Support Contacts at any time during the term of a Subscription by notifying ArkCase in writing and giving ArkCase five (5) business days to process the change. Technical Support Contacts will be the only interface to the ArkCase customer support center. It is recommended that the Technical Support Contacts be ArkCase certified by attending the required ArkCase training courses. In an emergency, an ArkCase customer support engineer will respond to an issue for an unauthorized contact on an exception basis subject to later verification and involvement of a named Technical Support Contact.