Commonwealth of Virginia
Virginia Information Technologies Agency

ADVANCED AUTHENTICATION PRODUCT INFORMATION TECHNOLOGY SOLUTION CONTRACT

Date: January 26, 2016

Contract #: VA-130131-CA

Authorized Users: All public bodies, including VITA, as defined by §2.2-4301 and referenced by §2.2-4304 of the *Code of Virginia*

Contractor:
CA, Inc.
One CA Plaza
Islandia, NY 11749
Website: http://www.ca.com

Contact:
Rene Hruska
2291 Wood Oak Drive
Care of SLED
Herndon, VA 20171
Phone: 216-798-8903
Email: Rene.Hruska@ca.com

FIN: 13-2857434

Term: January 31, 2016 – January 30, 2017

Payment: Net 30 days

For Additional Information, Please Contact:

Virginia Information Technologies Agency
Supply Chain Management

Mike Novak
Phone: 804-416-6168
Fax: 804-416-6361
E-Mail: mike.novak@vita.virginia.gov

NOTES: Individual Commonwealth of Virginia employees are not authorized to purchase products or services for their personal use from this Contract.

For updates, please visit our Website at http://www.vita2.virginia.gov/procurement/contracts.cfm

VIRGINIA INFORMATION TECHNOLOGIES AGENCY (VITA): Prior review and approval by VITA for purchases in excess of $100,000.00 is required for State Agencies and Institutions only.

CONTRACT #VA-130131-CA
CONTRACT CHANGE LOG

Change No.	Description of Change	Effective Date
1	Mod 1 adds clauses to clarify/define certain terminology used in the contract	07/24/14
2	Renewal letter extends contract term for a year	01/31/16
3	Updated Supplier's contact information	01/26/16

COMMONWEALTH of VIRGINIA

Virginia Information Technologies Agency
11751 Meadowville Lane
Chester, Virginia 23836-6315
(804) 416-6100

Nelson P. Moe
Chief Information Officer
Email: cio@vita.virginia.gov

TDD VOICE -TEL. NO.
711

December 10, 2015

Bruce Bryant
CA Technologies Inc.
One Ca Plaza
Islandia New York 11749

Mr. Bryant,

Per Section 3.A. ("Term and Termination") of contract VA-130131-CA, The Virginia Information Technologies Agency has elected to exercise its option to renew the contract for one year, from January 31, 2016 through January 30, 2017. Should you have any questions, please feel free to contact me.

Respectfully,
Doug Crenshaw
Strategic Sourcing Manager
Virginia Information Technologies Agency
(804) 416-6160

MODIFICATION NO. 1
TO
CONTRACT NUMBER VA-130131-CA
BETWEEN THE
COMMONWEALTH OF VIRGINIA
AND
CA, INC.

This MODIFICATION No. 1 is hereby incorporated into and made an integral part of Contract VA-130131-CA

The purpose of this Modification is to add the clause(s) and clarifications listed below:

1. Add to the definition of "Authorized Users" in Section 2 Subsection C on Contract Page 5.

   "Authorized Users also include private institutions of higher education chartered in Virginia and granted tax-exempt status under §501(c)(3) of the Internal Revenue Code. A list of the private institutions eligible to use this contract can be found at http://www.cicv.org/our-Colleges/Profiles.aspX

2. Add to the definition of "Software License" in Section 4 on Contract Page 9.

   "If Authorized User is a state agency, board, commission, or other quasi-political entity of the Commonwealth of Virginia or other body referenced in Title 2.2 of the Code of Virginia, the license shall be held by the Commonwealth. If Authorized User is a locality, municipality, school, school system, college, university, local board, local commission, or local quasi-political entity, the license shall be held by that public body. *If Authorized User is a private institution, the license shall be held by that private institution."*

3. Add to the definition of "Rights to Work Product" in Section 5 on Contract Page 11.

   "If Authorized User is a private institution of higher education chartered in Virginia and granted tax-exempt status under §501(c)(3) of the Internal Revenue Code, any license to private institution's pre-existing work shall be held by, and all rights in, title to, and ownership of private institution's Work Product shall vest with that institution."

4. Add to the definition of "Software and Deliverable Acceptance Criteria" in Section 9 Subsection A on Contract Page 15.

   "If the Authorized User is a private institution chartered in Virginia and granted tax-exempt status under §501(c)(3) of the Internal Revenue Code, such private institution may have its own per diem amounts applicable to Supplier's pre-approved travel expenses."

5. Add to the definition of "Dispute Resolution" in Section 24 Subsection E on Contract Pages 26.

   "In the event of any breach by a public body *or a private institution*, Supplier's remedies shall be limited to claims for damages and Prompt Payment Act interest and, if available and warranted, equitable relief, all such claims to be processed pursuant to this Section. In no event shall Supplier's remedies include to the right to terminate any license or support services hereunder."

The foregoing is the complete and final expression of the parties' agreement to modify Contract VA-130131-CA by this Modification No. 1.

ALL OTHER TERMS AND CONDITIONS REMAIN UNCHANGED.

PERSONS SIGNING THIS CONTRACT ARE AUTHORIZED REPRESENTATIVES OF EACH PARTY TO THIS CONTRACT AND ACKNOWLEDGE THAT EACH PARTY AGREES TO BE BOUND BY THE TERMS AND CONDITIONS OF THE CONTRACT.

CA, Inc.
BY: Ann Michele Costello
NAME: Ann Michele Costello
Sr. Director - Contracts
TITLE:
DATE: 24 July 2014

COMMONWEALTH OF VIRGINIA
BY: Doug Crenshaw
NAME: Doug Crenshaw
TITLE: VITA Sourcing Mgr
DATE: 7/24/14

Advanced Authentication Product Information Technology Solution Contract

between

The Virginia Information Technologies Agency

on behalf of

The Commonwealth of Virginia

and

CA, INC.

AAP INFORMATION TECHNOLOGY SOLUTION CONTRACT
TABLE OF CONTENTS

AAP INFORMATION TECHNOLOGY SOLUTION CONTRACT

THIS ADVANCED AUTHENTICATION PRODUCT INFORMATION TECHNOLOGY SOLUTION CONTRACT ("Contract") is entered into by and between the Virginia Information Technologies Agency ("VITA" or "Customer") pursuant to §2.2-2012 of the Code of Virginia and on behalf of the Commonwealth of Virginia, (hereinafter referred to as "VITA") and _CA, Inc.("CA" or "Supplier"), a corporation headquartered at One CA Plaza, Islandia, NY, 11749, USA, to be effective as of January 31, 2013 (Effective Date).

1. PURPOSE

This Contract sets forth the terms and conditions under which Supplier agrees to provide and implement for Authorized Users a solution for Advanced Authentication Products ("Solution"), and to provide various Services to the Authorized Users.

2. DEFINITIONS

A. Acceptance

Successful performance of the Solution at the location designated in the applicable Statement of Work, or completed and successful Acceptance testing in conformance with the Requirements as determined by the Authorized User in the applicable Statement of Work.

B. Agent

Any third party independent agent of any Authorized User, subject to the Agent's compliance with the terms of this Contract.

C. Authorized Users

All public bodies, including VITA, as defined by §2.2-4301 and referenced by §2.2-4304 of the Code of Virginia.

D. Authorized Use Limitations

Means the quantity of the Supplier Software licensed in accordance with the License Metric specified on the Statement of Work.

E. CA Documentation

Means the documentation, technical product specifications and/or user manuals as defined in Exhibit I.

F. CA Offering

Means the individual offering (such as software, services, software as a service etc.) made available by Supplier as defined in the Contract and/or order.

G. Commonwealth Intellectual Property

Means Confidential Information and any business requirements, materials, information and/or intellectual property owned or licensed that is provided by the Commonwealth, which includes, without limitation all patents, copyrights, trademarks, trade secrets, and other intellectual property rights that may be accessed or used during the provision of Services but in all cases excludes any Supplier Intellectual Property

H. Computer Virus

Any malicious code, program, or other internal component (e.g., computer virus, computer worm, computer time bomb, or similar component), which could damage, destroy, alter or disrupt any computer program, firmware, or hardware or which could, in any manner, reveal, damage, destroy, alter or disrupt any data or other information accessed through or processed by such Software in any manner.

I. Confidential Information

Any confidential or proprietary information of a Party that is disclosed in any manner, including oral or written, graphic, machine readable or other tangible form, to any other Party in connection with or as a result of discussions related to this Contract or any order or Statement of Work issued hereunder, and which at the time of disclosure either (i) is marked as being “Confidential” or “Proprietary”, (ii) is otherwise reasonably identifiable as the confidential or proprietary information of the disclosing Party, or (iii) under the circumstances of disclosure should reasonably be considered as confidential or proprietary information of the disclosing Party.

J. Deliverable
The tangible embodiment of the Services, , performed or the Solution or Solution component provided by Supplier as identified in the applicable Statement of Work.

K. Distributed
Distributed means the CA Software designated as distributed that is generally used for indepedent usage across individuals systems or hardware based on the Licensed Metric in a decentralized form of computing.

L. Documentation
Those materials detailing the information and instructions needed in order to allow any Authorized User and its Agents to make productive use of the Solution, and to implement and develop self-sufficiency with regard to the Solution as may be specified in a Statement of Work issued hereunder.

M. Education
Means any standard or customized education offerings, training or instruction, or related services, provided by CA or a CA subcontractor in any format or location, including without limitation, (i) instructor led training, including at CA or Authorized User site(s), (ii) virtual training, including online classes, courses, or course catalogues and/or (iii) class room training or testing, at a CA or third party training facility.

N. Electronic Self-Help
Any use of electronic means to exercise Supplier’s license termination rights, if allowable pursuant to the Software License section of this Contract, upon breach or cancellation, termination or expiration of this Contract or any order placed hereunder.

O. License Metric
Means the specific criteria for measuring the usage of the CA Software (such as MIPS, CPUs, tiers, servers, or users).

P. Mainframe
Means CA Software designated as mainframe that is generally used for a large capacity processor that provides links to users through less powerful devices such as workstations or terminals based on the Licnesed Metric in a centralized form of computing

Q. Maintenance
Means the provision of new Releases made available while on active Support or new Versions if applicable to the generally available Supplier Software licensed by Authorized User.

R. Party
Supplier, VITA, or any Authorized User.

S. Receipt
An Authorized User or its Agent has physically received any deliverable at the correct “ship-to” location.

T. Perpetual License
Means a license that is paid in full by VITA to use Supplier Software for an indefinite period.

U. Requirements
The functional, performance, operational, compatibility, Acceptance testing criteria and other parameters and characteristics of the Service(s) and Deliverables as set forth in Exhibit A and the applicable Statement of Work and such other parameters, characteristics, or performance standards that may be agreed upon in writing by the Parties.

V. Release

Means a general available release of a Supplier Software, which may contain minor new Software product functionality, code, or compatibility and incorporates all previous fixes (if any exist) since the last Version. Typically, a Release requires a new installation, rather than an overlay to the already installed Software. Unless otherwise specified by Supplier for a particular product, a Release is tied to the preceding Version and is typically designated by a number to the right of the decimal point such as 1.1, 1.2, 1.3, etc.

W. Services

“Services" means the professional services provided by Supplier or its designated subcontractors to the Authorized User as set out in the relevant SOW.

X. Software

Means the computer software programs, either provided individually or packaged as a Software appliance, made generally available and licensed to an Authorized User under a Contract pursuant to the applicable order including all Versions, Releases, provided as part of Support if applicable.

Y. Software Publisher

The licensor of the Software provided by Supplier under this Contract.

Z. Statement of Work (SOW)

Any document in substantially the form of Exhibit D which will include Supplier’s Order Form (Exhibit H) (describing the deliverables, due dates, assignment duration and payment obligations for a specific project, engagement, or assignment for which Supplier shall be providing a Solution and/or Services to an Authorized User), which, upon signing by both Parties, shall be deemed a part of this Contract.

AA. Supplier

Means the Supplier and any of its Affiliates (i.e., an entity that controls, is controlled by, or is under common control with Supplier).

BB. Support

Means the provision of technical support and Maintenance provided for a particular Supplier Software as further defined in the Contract or order.

CC. Version

Means a release of a Supplier Software Product that contains major changes in Software product functionality, code, or compatibility and incorporates the previous release (if one has occurred), fixes and service Packs (if they have occurred). Typically, a Version requires a new installation, rather than an overlay to the already installed Software. Unless otherwise specified by Supplier for a particular product, a Version is designated by the number to the left of the decimal point such as 1.0, 2.0, 3.0, etc.

DD. Work Product

Inventions, combinations, machines, methods, formulae, techniques, processes, improvements, software designs, computer programs, strategies, specific computer-related know-how, data and original works of authorship (collectively, the "Work Product") discovered, created, or developed by Supplier, or jointly by Supplier and an Authorized User(s) in the performance of this Contract or any order issued hereunder. Work Product shall not include configuration of Software.

3. TERM AND TERMINATION

A. Contract Term

This Contract is effective and legally binding as of the Effective Date and, unless terminated as provided for in this section, shall continue to be effective and legally binding for a period of three (3) years. VITA, in its sole discretion, may extend this Contract for up to five (5) additional one (1) year periods after the expiration of the initial three (3) year period. VITA will issue a written notification to the Supplier stating the extension period thirty (30) days prior to the expiration of any current term. In addition, performance of an order or SOW issued during the term of this Contract may survive the expiration of the term of this Contract, in which case all terms and conditions required for the operation of such order or SOW shall remain in full force and effect until the Solution and all Services pursuant to such order or SOW have met the final Acceptance criteria of the applicable Authorized User.

B. Termination for Convenience

VITA may terminate this Contract, in whole or in part, or any order or SOW issued hereunder, in whole or in part, or an Authorized User may terminate an order or SOW, in whole or in part, upon not less than thirty (30) days prior written notice at any time for any reason.

C. Termination for Breach or Default

VITA shall have the right to terminate this Contract, in whole or in part, or any order or SOW issued hereunder, in whole or in part, or an Authorized User may terminate an order or SOW, in whole or in part, for breach and/or default of Supplier. Supplier shall be deemed in breach and/or default in the event that Supplier fails to meet any material obligation set forth in this Contract or in any order or SOW issued hereunder.

If VITA deems the Supplier to be materially in breach and/or default, VITA shall provide Supplier with notice of breach and/or default and allow Supplier fifteen (15) days to cure the breach and/or default If Supplier fails to cure the breach as noted, VITA may immediately terminate this Contract or any order or SOW issued hereunder, in whole or in part. If an Authorized User deems the Supplier to be materially in breach and/or default in accordance with the order or SOW, such Authorized User shall provide Supplier with notice of breach and/or default and allow Supplier fifteen (15) days to cure the breach and/or default. If Supplier fails to cure the breach and/or default as noted, such Authorized User may immediately terminate its order or SOW, in whole or in part. Any such termination shall be deemed a Termination for Breach or Termination for Default. In addition, if Supplier is found by a court of competent jurisdiction to be in violation of or to have violated 31 USC 1352 or if Supplier becomes a party excluded from Federal Procurement and Nonprocurement Programs, VITA may immediately terminate this Contract, in whole or in part, for breach, and VITA shall provide written notice to Supplier of such termination. Supplier shall provide prompt written notice to VITA if Supplier is charged with violation of 31 USC 1352 or if federal debarment proceedings are instituted against Supplier.

D. Termination for Non-Appropriation of Funds

All payment obligations under this Contract are subject to the availability of legislative appropriations at the federal, state, or local level, for this purpose. In the event of non-appropriation of funds, irrespective of the source of funds, for the items under this Contract, VITA may terminate this Contract, in whole or in part, or any order, in whole or in part, or an Authorized User may terminate an order, in whole or in part, for those goods or services for which funds have not been appropriated. Written notice will be provided to the Supplier as soon as possible after legislative action is completed.

E. Effect of Termination

Termination of this Contract will not result in termination of an Authorized User’s order or SOW and such terms shall survive until such time the SOW or order expires or is otherwise terminated.

Termination does not release either Party from any liability which, at the time of such termination, had already been accepted by the other party.nor preclude either Party from pursuing any rights or remedies it may have under law or in equity with respect to any breach of this Contract. Upon termination for any reason, Authorized User shall pay Supplier any fees and expenses accepted by Authorized User under the applicable SOW or order whether due before or after the date of termination which shall become immediately due and payable to Supplier on such termination.

Upon termination, neither the Commonwealth, nor VITA, nor any Authorized User shall have any future liability except for Deliverables accepted by the Authorized User or Services rendered by Supplier and accepted by the Authorized User through the termination date.

In the event of a Termination for Breach or Termination for Default, Supplier shall accept return of any Deliverable that was not accepted by the Authorized User(s), and Supplier shall refund any monies paid by any Authorized User for such Deliverable, and all costs of de-installation and return of Deliverables shall be borne by Supplier.

F. Transition of Services

Prior to or upon expiration or termination of this Contract and at the request of VITA, Supplier shall provide all assistance as VITA or an Authorized User may reasonably require to transition Solution-related Services to any other supplier with whom VITA or such Authorized User contracts for provision of a solution(s). This obligation may extend beyond expiration or termination of the Contract for a period not to exceed six (6) months. In the event of a termination for breach and/or default of Supplier, Supplier shall provide such assistance at no charge or fee to VITA or any Authorized User; otherwise, Supplier shall provide such assistance at the hourly rate or a charge agreed upon by Supplier and VITA or an Authorized User.

G. Contract Kick-Off Meeting

Within 30 days of Contract award, Supplier may be required to attend a contract orientation meeting, along with the VITA contract manager/administrator, the VITA and/or other CoVa Agency project manager(s) or authorized representative(s), technical leads, VITA representatives for SWaM and Sales/IFA reporting, as applicable, and any other significant stakeholders who have a part in the successful performance of this Contract. The purpose of this meeting will be to review all contractual obligations for both parties, all administrative and reporting requirements, and to discuss any other relationship, responsibility, communication and performance criteria set forth in the Contract. The Supplier may be required to have its assigned account manager as specified in Section 6.0 and a representative from its contracts department in attendance. The time and location of this meeting will be coordinated with Supplier and other meeting participants by the VITA contract manager.

H. Contract Closeout

Prior to the contract's expiration date, Supplier may be provided contract close out documentation and shall complete, sign and return to VITA Supply Chain Management within 30 days of receipt. This documentation may include, but not be limited to: Patent/Royalty Certificate, Tangible Property/Asset Certificate, Escrow Certificate, SWaM Reports Completion Certificate, Sales Reports/IFA Payments Completion Certificate, and Final Payment Certificate. Supplier is required to process these as requested to ensure completion of close-out administration and to maintain a positive performance reputation with the Commonwealth of Virginia. Any closeout documentation not received within 30 days of Supplier's receipt of our request will be documented in the contract file as Supplier non-compliance. Supplier's non-compliance may affect any pending payments due the Supplier, including final payment, until the documentation is returned.

4. SOFTWARE LICENSE

If Authorized User is a state agency, board, commission, or other quasi-political entity of the Commonwealth of Virginia or other body referenced in Title 2.2 of the Code of Virginia, the license shall be held by the Commonwealth. If Authorized User is a locality, municipality, school, school system, college, university, local board, local commission, or local quasi-political entity, the license shall be held by that public body.

A. License Grant

The following license grant applies to the Commonwealth of Virginia/VITA and all Authorized Users therein and is used exclusively for the legitimate business and activities of the Commonwealth of Virginia.

Supplier grants to the Commonwealth and all Authorized Users a fully paid, perpetual, nonexclusive, transferable (to other VITA agencies and Agents), irrevocable license to use,, transmit and distribute the Software and Documentation including any subsequent revisions, in accordance with the terms and conditions set forth herein and subject only to the limitations and/or restrictions explicitly set forth in this Contract. It is expressly understood that "perpetual" license rights shall commence upon delivery of the Software to the Authorized User and shall exist in perpetuity unless otherwise terminated in accordance with the applicable provisions of the Contract. The Software is the property of Supplier, and no title or ownership of the Software or any of its parts, including Documentation, shall transfer to the Commonwealth or any Authorized User.

The Commonwealth and all Authorized Users shall have the right to use, , , transmit and distribute the Software for their benefit, for government use and purposes, and for the benefit of their Agents, including internal and third-party information processing.

The Commonwealth and any Authorized User may allow access to the Software by third party vendors who are under contract with an Authorized User to provide services to or on behalf of such Authorized User, or by other entities as required for conducting the business of government. Access includes loading or executing the Software on behalf of such Authorized Users or their Agents.

The license fee includes a test system copy, which consists of the right to use the Software for non-production test purposes, including but not limited to, problem/defect identification, remediation, and resolution, debugging, new version evaluation, Software interface testing, and disaster recovery technique analysis and implementation.

In the event that all of an Authorized User’s copies of the Software, including all backup copies, are destroyed, irreparably damaged or otherwise lost due to fire, explosion, sabotage, flood or other disaster, Supplier shall provide to such Authorized User, at no additional cost, replacement copies of the Software and Documentation. Nothing contained in this Section shall obligate Supplier to replace or assist in the recovery of data lost concurrent with the loss of the Software.

An Authorized User may make a reasonable number of copies of the Supplier Software for disaster recovery “cold standby”, backup and archival purposes. Use of such copies is limited to testing Authorized User’s disaster recovery procedures and effectiveness and as is necessary during any reasonable period subsequent to the occurrence of an actual disaster during which Authorized User cannot operate the Supplier Software.

Except as expressly authorized, an Authorized User shall not distribute the Software to any third party without Supplier’s prior written consent.

Authorized User may relocate Supplier Software to a new Authorized User location within the Commonwealth upon prior written notice.

The Supplier Software's specifications and specified operating environment information may be found in the Documentation accompanying the Supplier Software, if available (e.g., a user manual, user guide, or readme.txt or notice.txt file).

Upon request by Supplier, Authorized User agrees to provide records reasonably requested by Supplier to verify its compliance with the Authorized Use Limitation defined in the SOW during the period in which Authorized User is licensed to use the Software and for a period of twelve (12) months after expiration including certified copies of statements or records as applicable. Such reports will be based on the License Metric indicated on the SOW.

The grant of license is contingent upon Authorized User’s compliance with the following obligations set out under this provision: Authorized User agrees, that it shall not: (i) access or use any portion of the Supplier Software not expressly authorized in the SOW or the Documentation of the Supplier Software; (ii) cause or permit de-compilation, reverse engineering, or otherwise translate all or any portion of the Supplier Software; (iii) modify, unbundle, or create derivative works of the Supplier Software and/or Documentation; (iv) rent, sell, lease, assign, transfer or sublicense the Supplier Software to provide hosting, service bureau, on demand or outsourcing services for the benefit of a third party; (v) remove any proprietary notices, labels, or marks on or in any copy of the Supplier Software or Documentation; (vi) use the Supplier Software beyond the Authorized Use Limitation.

Supplier reserves the right, with reasonable mutually agreed upon notice to the Authorized User, to conduct an audit remotely or onsite of Authorized User and/or its Affiliates facilities to verify Authorized User’s compliance with the terms of the Contract. Supplier agrees that such audit shall be conducted during regular business hours at Authorized User's offices and Supplier shall endeavor to conduct such audit so as not to interfere unreasonably with Authorized User's activities and/or use an independent third party to conduct the audit subject to terms of non-disclosure if required. The Authorized User reserves the right to be present during the audit.

Such audit to be conducted once per year or as otherwise mutually agreed.

All rights not specifically granted hereunder are expressly reserved.

Nothing contained herein shall be construed to restrict or limit the rights of the Commonwealth or any Authorized User to use any technical data, which the Commonwealth or such Authorized User may already possess or acquire under proper authorization from other sources.

Compliance with the terms and conditions of any license granted pursuant to this Contract is solely the responsibility of the Authorized User which purchased such license or for which such license was purchased and not the responsibility of VITA, unless VITA purchased such license on its own behalf.

B. License Type

All licenses granted, regardless of the type, include all uses set forth above. License type may vary by Software product and shall be set forth in Exhibit B and identified on any order issued pursuant to this Contract

- **Perpetual**. The licensee pays a one-time license fee and has the right to use the Licensed Program for an indefinite period of time. Maintenance and enhancement services are provided at an additional annual maintenance fee. The licensee may use the perpetual license indefinitely with no additional payments after the one-time fee is paid.
- **Subscription**. The licensee has the right to usage and maintenance of the Licensed Program during the specific term (i.e. 3 years) of the agreement. Thereafter, the parties will mutually agree to renew on the same terms and conditions, but subject to Licensee's payment of CA's then prevailing subscription license fee.
- **Unlimited Term License**: The licensee can deploy an unlimited number of users over the three (3) year term. Sixty (60) days prior to the end of the 3 year term, the Commonwealth will report/count the number of users in production and submit that number to CA. That number (active users at the end of the 3 yr term) will be converted to a traditional Perpetual license.

5. RIGHTS TO WORK PRODUCT

Supplier retains all right, title, copyright, patent, trademark, trade secret and all other proprietary interests to all Supplier software, documentation, services, educational training("CA Offerings") and any derivatives thereof (Work Product). No title, copyright, patent, trademark, trade secret or other right of intellectual property not expressly granted under the Contract is exchanged between the Parties.

Commonwealth shall retain all rights in and to Commonwealth Intellectual Property, including all Commonwealth Intellectual Property that may be contained in the Deliverables, and such rights shall remain vested in the Commonwealth.

Supplier shall retain all rights in and to all Supplier Intellectual Property and such rights shall remain vested in Supplier.

If information or materials are used by a party in the performance of its obligations in the Contract, such use of information or materials shall not transfer ownership of that information or materials to the other party.

Supplier grants to Commonwealth, a non-exclusive, limited, transferable within the Commonwealth, the license to use the Deliverables and Modifications, (including Work Product) for internal business purposes subject to terms of the Contract. Where the Deliverables or Modifications are to be used in conjunction with Supplier Software then the license to use the Deliverables or Modifications shall be consistent with the usage limitations as set out in the license agreement for such Supplier Software.

.

A. Return of Materials

Upon termination of this Contract, Supplier shall immediately return to VITA or the appropriate Authorized User all copies, in whatever form, of any and all Confidential Information, Commonwealth Intellectual Property and other properties provided by VITA or such Authorized User, which are in Supplier's possession, custody or control.

6. SUPPLIER PERSONNEL

A. Selection And Management Of Supplier Personnel

Supplier shall take such steps as may be necessary to ensure that all Supplier personnel performing under this Contract are competent and knowledgeable of the contractual arrangements and the applicable SOW between Authorized User and Supplier. Supplier shall be solely responsible for the conduct of its employees, agents, and subcontractors, including all acts and omissions of such employees, agents, and subcontractors, and shall ensure that such employees and subcontractors comply with the appropriate Authorized User's site security, information security and personnel conduct rules, as well as applicable federal, state and local laws, including export regulations. Authorized User reserves the right to require the immediate removal from such Authorized User's premises of any employee, subcontractor or agent of Supplier whom such Authorized User believes has failed to comply or whose conduct or behavior is unacceptable or unprofessional or results in a security or safety breach.

B. Supplier Personnel Supervision

Supplier acknowledges that Supplier, or any of its agents, contractors, or subcontractors, is and shall be the employer of Supplier personnel, and shall have sole responsibility to supervise, counsel, discipline, review, evaluate, set the pay rates of and terminate the employment of Supplier personnel.

C. Key Personnel

An SOW may designate certain of Supplier's personnel as Key Personnel or Project Managers. Supplier's obligations with respect to Key Personnel and Project Managers shall be described in the applicable SOW. Failure of Supplier to perform in accordance with such obligations may be deemed a default of this Contract or of the applicable SOW.

D. Subcontractors

Supplier shall not use subcontractors to perform the Services unless specifically authorized in writing to do so by the Authorized User, which authorization shall not be unreasonably withheld. If an order or SOW issued pursuant to this Contract is supported in whole or in part with federal funds, Supplier shall not subcontract any Services pursuant to such order or SOW to any subcontractor that is a party excluded from Federal Procurement and Nonprocurement Programs. In no event shall Supplier subcontract any Services to any subcontractor which is debarred by the Commonwealth of Virginia or which owes back taxes to the Commonwealth and has not made arrangements with the Commonwealth for payment of such back taxes.

7. GENERAL WARRANTY

Supplier warrants and represents to VITA the Solution described in Exhibit A as follows:

A. Ownership

Supplier has the right to provide the Solution without violating or infringing any law, rule, regulation, copyright, patent, trade secret or other proprietary right of any third party.

B. Solution

During the Warranty Period of ninety (90) days, or as specified in the applicable SOW, Supplier warrants that the Solution will be in accordance with its responses to the Requirements. Supplier shall correct at no additional cost to any Authorized User, all errors identified during the Warranty Period that result in a failure to meet the Requirements. Should Supplier not be able to repair or replace the defective software or re-perform the Services within the Warranty Period, the Authorized User's sole and exclusive remedy will be a refund of any fees that have been accepted and paid and to terminate the SOW for convenience. The Warranty remedies are conditioned upon (i) any error or defect complained of is reasonably reproducible by Supplier, (ii) the Supplier Software is not adapted or modified and is being used in accordance with Requirements and the CA Documentation, and (iii) the breach is not attributable in whole or in part to any non-Supplier product(s) or service(s).

C. Malicious Code
Anti-Virus Warranty:

The Supplier warrants that it will use all reasonable efforts to verify that Software supplied by the Supplier to Authorized User pursuant to this Contract shall be virus free at time of delivery to Authorized User. Notwithstanding the aforementioned warranty, Authorized User agrees that upon receipt of Software it will take all reasonable industry standard measures prior to loading the Software onto a production environment including but not restricted to the use of reputable virus checking software to verify that the Software is free of known viruses. In the event that a virus is found to exist on the Software, Authorized User shall inform the Supplier within seventy-two (72) hours of finding the virus and shall not allow use of affected Software for any purpose whatsoever.

In the event of a breach of this Warranty, VITA's remedy is for Supplier, in consultation with VITA, to (i) use reasonable efforts consistent with industry standards to cure the defect (i.e remove the virus), or (ii) replace the Supplier Software(s) with one that is virus-free or (iii) if (i) and (ii) are not commercially feasible and if the parties mutually agree, terminate the license and provide a pro-rata refund of the license fees paid and or Support fees. If option (iii) applies, the pro-rata refund shall be calculated on the number of months left remaining on the Term of the applicable SOW or if the Supplier Software is licensed under a Perpetual License, using (only for purposes of a refund calculation) an amortization schedule of three (3) years.

D. Warranty against "Harmful Code" (Worms, Trojans etc):
In this Section, "Harmful Code" shall mean any software code constructed with the ability to damage, interfere with, or adversely affect computer programs, data files, or hardware without the consent or intent of the computer user. This definition includes, but is not limited to, self-replacing and self-propagating programming instructions commonly called "viruses," "trojan horses" and "worms". Supplier warrants that it will use all reasonable efforts to verify that software supplied by Supplier to Authorized User pursuant to this Agreement shall at the time of despatch to Authorized User be free from Harmful Code and, in the case of non-evaluation software or beta testing Software shall be free from disabling devices which would (i) enable Supplier to remotely de-install the Software or (ii) ensure the Software will function only for a limited period of time, provided in all cases that (a) the Software is not modified by anyone other than Supplier, unless authorized by Supplier in writing; (b) Authorized User notifies Supplier in writing of the nonconformity within the term of the license for Subscription Software or within the Support period for Perpetual Software and (c) the Software is installed in a compatible environment. Notwithstanding the aforementioned warranty, Authorized User agrees that upon receipt of Software, and prior to loading onto a production environment, Authorized User will take all reasonable measures including but not restricted to the use of reputable virus checking software to ensure the Software received by Authorized User is free of known Harmful Code. In the event that Harmful Code is found to exist on the Software, Authorized User shall inform Supplier within seventy-two (72) hours of finding the same and shall not allow use of affected Software for any purpose whatsoever. Authorized User's sole remedy under this Section is for Supplier at its option to provide a copy of Software free of Harmful Code or upon mutual agreement of the parties, to refund to Authorized User the consideration paid for such Software upon return of all of the Software. In the event of a refund, Authorized User's right to use the Software shall automatically expire.

The foregoing warranty of Supplier notwithstanding, Authorized User understands and agrees that certain of Supplier's software programs contain passwords or similar devices which require renewal for continued operation, and that, provided Supplier notifies Licensee in advance of the existence of such passwords or devices, the use of such passwords or devices, is not restricted or prohibited by the terms of this provision.

Supplier has used commercially feasible efforts through quality assurance procedures to ensure that there are no Computer Viruses or undocumented features in the Solution at the time of delivery to an Authorized User. Supplier warrants that the Solution does not contain any embedded device or code (e.g., time bomb) that is intended to obstruct or prevent any Authorized User's use of the Solution. Notwithstanding any rights granted under this Contract or at law, Supplier hereby waives under any and all circumstances any right it may have or may hereafter have to exercise Electronic Self-Help. Supplier agrees that an Authorized User may pursue all remedies provided under law in the event of a breach or threatened breach of this Section, including injunctive or other equitable relief.

E. Open Source

Supplier will notify all Authorized Users if the Solution contains any Open Source code and identify the specific Open Source License that applies to any embedded code dependent on Open Source code, provided by Supplier under this Contract.

F. Supplier's Viability

Supplier warrants that it has the financial capacity to perform and continue to perform its obligations under this Contract; that Supplier has no constructive or actual knowledge of a potential legal proceeding being brought against Supplier that could materially adversely affect performance of this Contract; and that entering into this Contract is not prohibited by any contract, or order by any court of competent jurisdiction.

THE OBLIGATIONS OF SUPPLIER UNDER THIS GENERAL WARRANTY SECTION ARE MATERIAL. THE ABOVE WARRANTIES ARE THE SOLE WARRANTIES PROVIDED BY SUPPLIER. NO OTHER WARRANTIES, INCLUDING THAT THE SUPPLIER SOFTWARE IS ERROR FREE, WHETHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT, OR SUITABILITY AND/OR THE WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE ARE MADE BY SUPPLIER OR ITS SUPPLIERS.

8. DELIVERY AND INSTALLATION

A. Scheduling

Supplier shall deliver the Solution, including any component parts, and complete performance of Services according to the delivery dates set forth on the appropriate order.

Supplier shall make available all appropriate and/or related Documentation at the time of delivery of the relevant component of the Solution. Any Solution component delivered without the appropriate and required Documentation shall be considered "shipped short" until the applicable documentation has been received.

The Software will be delivered by electronic delivery (ESD), as defined in INCOTERMS 2010, from Supplier's shipping point as indicated in the SOW. Supplier agrees to be responsible for all customs duties and clearances and title to any Supplier hardware if included will pass upon point of delivery to carrier at Supplier's shipping location

B. Deployment of Solution

Supplier Deployment of Solution

The Solution fee includes initial deployment of the complete Solution. Supplier is required to deploy the Solution in accordance with the deployment schedule set forth on the order. Deployment shall include the installation of any Software component and, if agreed, any hardware component, of the Solution. Supplier shall conduct its standard appropriate diagnostic evaluation at the Authorized User's user site to determine that the Solution is properly deployed and fully ready for productive use, and shall supply such Authorized User with a copy of the results of the diagnostic evaluation promptly after completion of deployment.

Supplier agrees that its sole failure to deploy the Solution, in accordance with the delivery schedule in the applicable order shall constitute a material breach of this Contract resulting in damages to such Authorized User.

C. Documentation of Software Configuration

If the Solution includes configuration of Software by Supplier, Supplier shall provide to the appropriate Authorized User documentation containing a description of the configuration. Such documentation shall be sufficiently detailed such that any appropriately trained employee or Agent of any Authorized User may reconstruct the configuration of the Software.

9. ACCEPTANCE

A. Software and Deliverable Acceptance Criteria

Software and Deliverables shall be deemed accepted when the Authorized User determines that such Software and Deliverables successfully operate in accordance with the Requirements. At a minimum, Acceptance Criteria for Software and Deliverables, and for the Solution as a whole, shall ensure that all of the functionality described in the Requirements set forth in Exhibit A and required by the Authorized User in the applicable SOW has been delivered to the Authorized User. Acceptance of any one Deliverable shall not imply Authorized User's concurrence that the Deliverable will function properly with or within the Solution. Supplier shall be responsible for ensuring that all Deliverables function properly within the Solution. Should a previously Accepted Deliverable require further modification in order to work properly with or within the Solution, Supplier shall be responsible for all costs associated with such modification.

Such Authorized User agrees to commence Acceptance testing within ten (10) days, or within such other period as set forth in the applicable SOW, after receipt of the Software or Deliverable. Acceptance testing will be no longer than forty-five (45) days, or such other period as may be agreed in writing between Authorized User and Supplier, for the first instance of each product type set forth in Exhibit B. Supplier agrees to provide to such Authorized User such assistance and advice as such Authorized User may reasonably require, at no additional cost, during such Acceptance testing, other than pre-approved travel expenses for fixed price type SOWs in which travel expenses were expressly excluded from the total price of the SOW. Any such travel expenses must be pre-approved by the Authorized User and shall be reimbursable by such Authorized User at the then-current per diem amounts as published by the Virginia Department of Accounts (http://www.doa.virginia.gov), or a successor URL(s)). Authorized User shall provide to Supplier written notice of Acceptance upon completion of successful Acceptance testing. Should Authorized User fail to provide Supplier written notice of successful or unsuccessful Acceptance testing within five (5) days, or as otherwise specified in the SOW following the Acceptance testing period, the Service shall be deemed Accepted.

B. Software and Deliverable Cure Period

Supplier shall correct any non-conformities identified during Acceptance testing and re-submit such non-conforming Software or Deliverable for re-testing within fifteen (15) days of the appropriate Authorized User's written notice of non-conformance, or as otherwise agreed between such Authorized User and Supplier in the applicable SOW. Should Supplier fail to cure the non-conformity or deliver Software or a Deliverable which meets the Requirements, such Authorized User may, in its reasonable discretion: (i) reject the Software or Deliverable in its entirety and recover amounts previously paid hereunder; (ii) issue a "partial Acceptance" of the Software or Deliverable with an equitable adjustment in the price to account for such deficiency; or (iii) conditionally accept the applicable Software or Deliverable while reserving its right to revoke Acceptance if timely correction is not forthcoming. Failure of the Software or a Deliverable to meet, in all material respects, the Requirements after the second set of acceptance tests shall constitute a default by Supplier. In the event of such default, the Authorized User may, at its sole discretion, terminate its order or SOW, in whole or in part, for the Solution to be provided thereunder by Supplier.

C. Solution Acceptance Criteria

Solution shall be deemed accepted when the Authorized User determines that such Solution successfully operates in accordance with the mutually agreed upon Acceptance Test criteria set forth in the SOW.. Such Authorized User agrees to commence Acceptance testing within fifteen (15) days after deployment of the Solution. Acceptance testing will be completed within sixty (60) days, or such other period as may be agreed in writing between Authorized User and Supplier, after deployment of the Solution. Supplier agrees to provide to such Authorized User such assistance and advice as such Authorized User may reasonably require, at no additional cost, during such Acceptance testing, other than pre-approved travel expenses for fixed price type SOWs in which travel expenses were expressly excluded from the total price of the SOW. Any such travel expenses must be pre-approved by the Authorized User and shall be reimbursable by such Authorized User at the then-current per diem amounts as published by the Virginia Department of Accounts http://www.doa.virginia.gov, or a successor URL(s)). Authorized User shall provide to Supplier written notice of Acceptance upon completion of successful Acceptance testing. Should Authorized User fail to provide Supplier written notice of successful or unsuccessful Acceptance testing within five (5) days or as otherwise agreed upon in the SOW, following the Acceptance testing period, the Service shall be deemed Accepted.

D. Solution Cure Period

Supplier shall correct any non-conformities identified hereunder and shall thereafter re-submit such previously non-conforming Solution or component products or Services for re-testing within fifteen (15) days of written notice of non-conformance to Supplier, or as otherwise agreed between the Authorized User and Supplier. Should Supplier fail to deliver a Solution which meets the Requirements, such Authorized User may, in its reasonable discretion: (i) reject the Solution in its entirety and recover amounts previously paid hereunder; (ii) issue a “partial Acceptance” of the Solution with an equitable adjustment in the price to account for such deficiency; or (iii) conditionally accept the applicable Solution while reserving its right to revoke Acceptance if timely correction is not forthcoming. Failure of the Solution to meet, in all material respects, the specifications and performance standards after the second set of acceptance tests shall constitute a default by Supplier. In the event of such default, the Authorized User may, at its reasonable discretion, terminate its order, in whole or in part, for the Solution to be provided thereunder by Supplier.

10. WARRANTY AND MAINTENANCE SERVICES

At any time during the Warranty or Maintenance Period, as applicable, Supplier shall provide theSupport as set forth in the Support guidelines at **http://www.support.ca.com**. . During the Maintenance Period, charges shall be in accordance with this Section and Exhibit B.

A. Known Defects

Promptly make available to all Authorized Users in writing of any defects or malfunctions in the Solution or Documentation of which it learns from any source other than an Authorized User, correct any such defects or malfunctions or provide a work around until corrected, within five (5) days of Supplier’s knowledge of such defect or malfunction and provide all Authorized Users with corrected copies of same.

B. New Releases

Make available to all Authorized Users no later than the first day of general release, copies of the Software and Documentation revised to reflect any enhancements, including all new releases, upgrades, and access modes, to the Software made by Supplier, including, without limitation, modifications to the Software which can increase the speed, efficiency or base of operation of the Software or add additional capabilities to or otherwise improve the functionality of the Software.

C. Coverage

See CA support linkat: http://www.support.ca.com

D. Service Levels:

See support link at: http://www.support.ca.com

E. Software Evolution

Should Supplier or Software Publisher merge or splinter the Software previously provided to any Authorized User, such action on the part of Supplier or Software Publisher shall not in any way result in any Authorized User being charged additional license or support fees in order to receive enhancements, releases, upgrade or support for the Software.

If Supplier or Software Publisher reduces or replaces functionality contained in a licensed Software product and provides the same or substantially similar functionality as or within a separate or renamed Software product, then the Commonwealth or the Authorized User shall be entitled to license such Software product at no additional license or maintenance fee, and subject to the terms and conditions herein.

If Supplier or Software Publisher releases an option, future Software product or other release that has substantially the same functionality as the Software products provided under this Contract, and Software Publisher and/or Supplier ceases to provide maintenance for the older Software product, then Supplier shall offer the Commonwealth or the Authorized User the option to exchange licenses for such replacement Software product or function at no additional charge.

F. Escalation Procedures
To be detailed in the SOW.

G. Solution Support Services (Maintenance) and Renewal Options
Sixty (60) days prior to the expiration of the Maintenance Period, Supplier shall notify the Authorized User in writing of such expiration, and the Authorized User, at its sole discretion, may order from Supplier Solution support Services ("Maintenance Services"), including new Software releases, updates and upgrades, for a period of one (1) year ("Maintenance Period") at the fees set forth in Exhibit B. The annual fee for Maintenance shall not exceed the fee charged for the preceding year's Maintenance Services by more than three percent (3%), or the annual change in CPI, as defined in the Fees and Charges section, in effect at the time, whichever is less.

Supplier warrants that it shall, in accordance with Supplier's Support Policy and Terms at http://www.support.ca.com make Support Services available for all the Solution components listed in Exhibit B for a period of five (5) years from the expiration of the initial Warranty Period of any Solution provided to an Authorized User pursuant to this Contract. Cancellation of Maintenance Services by an Authorized User shall not affect this Contract or the grant of any license by Supplier.

11. TRAINING AND DOCUMENTATION
The Solution fee includes all costs for the training of one (1) Authorized User trainer per order or SOW at an Authorized User's designated location on the use and operation of the Solution. The Implementation classes will assist the Authorized User by instructing them how to install and configure the products. Pursuant to a mutually agreed upon schedule, Supplier shall provide personnel sufficiently experienced and qualified to conduct such training. Available optional training, and applicable pricing and discounts, are described in Exhibit B.

Supplier shall deliver to any Authorized User, one (1) hard copy or electronic media of Documentation, as requested by such Authorized User. Any Authorized User shall have the right, as part of the license granted herein, to make as many additional copies of the Documentation, in whole or in part, for its own use as required. This Documentation shall include, but not be limited to, overview descriptions of all major functions, detailed step-by-step operating procedures for each screen and activity, and technical reference manuals. All Authorized Users shall continue to include Supplier's copyright notice. The CA Documentation does not include Training Materials which are copyrighted and are not to be copied or duplicated by Authorized User.

A. EDUCATION OFFERING

- Supplier will provide Education as agreed in a SOW. The SOW will indicate the courses or classes ordered, the number of Attendees and the location of the Education services, if applicable. Authorized User is responsible for any travel costs and/or expenses incurred to attend Education.
- Supplier may require the registration or pre-registration of Authorized User's Attendees in order to attend or access the applicable Education. Authorized User acknowledges that Supplier has (or reserves) the right to refuse entry or access to any individual that cannot authenticate their registration or authorization for such Education. Any customized educational courses will be based on the rates and expenses of the instructor providing the course or such fees as stated in the SOW, as applicable.
- If Supplier cancels a class, due to unforeseen circumstances, or low enrollment, Supplier will provide as much advance notice as possible but no less than ten (10) business days prior to the

class in which case Authorized User may receive credit or reschedule the class to an alternative time

- If Authorized User elects to use the Supplier Education web access point to allow its Attendees to select and apply Education funds, Supplier will supply Authorized User with a PIN associated with the SOW. The PIN shall be used to help manage the expenditure of the Education funds and Authorized User will be responsible for (i) maintaining the confidentiality and proper use of that PIN by its Attendees designated to use such PIN and (ii) advising Supplier of such designated attendees.

Cancellation in writing by Authorized User must be provided at least ten (10) business days prior to the class. If such notice is not given Supplier may charge up to 100% of the fees for the class.

12. FEES, ORDERING AND PAYMENT PROCEDURE

A. Fees and Charges

As consideration for the Solution and any additional products and Services provided hereunder, an Authorized User shall pay Supplier the fee(s) set forth on Exhibit B, which lists any and all fees and charges. The fees and any associated discounts shall be applicable throughout the term of this Contract; provided, however, that in the event the fees or discounts apply for any period less than the entire term, Supplier agrees that it shall not increase the fees more than once during any twelve (12) month period, commencing at the end of year one (1). No such increase shall exceed the lesser of three percent (3%) or the annual increase in the Consumer Price Index for All Urban Consumers (CPI-U), U.S. City Average, All Items, Not Seasonally Adjusted, as published by the Bureau of Labor Statistics of the Department of Labor (http://www.bls.gov/cpi/home.htm), for the effective date of the increase compared with the same index one (1) year prior. Any such change in price shall be submitted in writing in accordance with the above and shall not become effective for sixty (60) days thereafter.

B. Solution Demonstration

At the request of any Authorized User, Supplier shall perform a demonstration of its Solution at such Authorized User's location and at no charge.

C. Statement of Work (SOW)

An SOW shall be required for any Solution ordered by an Authorized User pursuant to this Contract, along with Exhibit H. All Services shall be performed at the times and locations set forth in the applicable SOW and at the rates set forth in Exhibit B herein. Any SOW shall be of a fixed price type but may contain a cost-reimbursable line item(s) for pre-approved travel expenses.

Any change to an SOW must be described in a written change request (template provided as Exhibit E). Either Party to an SOW may issue a change request that will be subject to written approval of the other Party before it becomes part of this Contract. In no event shall any SOW or any modification thereto require the Supplier to provide any products or services that are beyond the scope of this Contract as such scope is defined in Exhibit A hereto.

D. Ordering

Notwithstanding all Authorized User's rights to license or purchase Supplier's products or services under this Contract, an Authorized User is under no obligation to purchase or license from Supplier any of Supplier's products or services. This Contract is optional use and non-exclusive, and all Authorized Users may, at their sole discretion, purchase, license or otherwise receive benefits from third party suppliers of products and services similar to, or in competition with, the products and services provided by Supplier.

Supplier is required to accept any order placed by an Authorized User through the eVA electronic procurement website portal (http://www.eva.virginia.gov/). eVA is the Commonwealth of Virginia's e-procurement system. State agencies, as defined in §2.2-2006 of the Code of Virginia, shall order through eVA. All orders placed will be based upon a mutually agreed upon SOW. Authorized Users may also place orders through the following means:

Purchase Order (PO): An official PO form issued by an Authorized User.

Any other order/payment charge or credit card process, such as AMEX, MASTERCARD, or VISA under contract for use by an Authorized User.

This ordering authority is limited to issuing orders for the Solution and products or Services related to the Solution available under this Contract. Under no circumstances shall any Authorized User have the authority to modify this Contract. An order from an Authorized User may contain additional terms and conditions; however, to the extent that the terms and conditions of the Authorized User's order are inconsistent with the terms and conditions of this Contract, the terms of this Contract shall supersede.

Notwithstanding the foregoing, Supplier shall not accept any order from an Authorized User if such order is to be funded, in whole or in part, by federal funds and if, at the time the order is placed, Supplier is not eligible to be the recipient of federal funds as may be noted on any of the Lists of Parties Excluded from Federal Procurement and Nonprocurement Programs.

ALL CONTRACTUAL OBLIGATIONS UNDER THIS CONTRACT IN CONNECTION WITH AN ORDER PLACED BY ANY AUTHORIZED USER ARE THE SOLE OBLIGATION OF SUCH AUTHORIZED USER AND NOT THE RESPONSIBILITY OF VITA UNLESS SUCH AUTHORIZED USER IS VITA.

E. Reserved

F. Invoice Procedures

Supplier shall remit each invoice to the "bill-to" address provided with the order promptly after all Solution, Solution component(s), or Services have been accepted and in accordance with the milestone payment schedule, if any, in the applicable order. Payment for Solution support Services shall be annually in arrears unless otherwise stated herein, or in any order referencing this Contract. No invoice shall include any costs other than those identified in the executed order, which costs shall be in accordance with Exhibit B. Without limiting the foregoing, all shipping costs are the Supplier's responsibility except to the extent such charges are identified in Exhibit B, or as noted in any executed order referencing this Contract. Invoices issued by the Supplier shall identify at a minimum:

Solution, product/Solution component, or Service type, or project milestone, and description

Quantity, charge and extended pricing for each Solution and/or Service item or milestone

Applicable order date

This Contract number and the applicable order number

Supplier's Federal Employer Identification Number (FEIN).

Any terms included on Supplier's invoice shall have no force or effect and will in no way bind VITA or any Authorized User.

G. Purchase Payment Terms

Supplier is responsible for the accuracy of its billing information. Supplier agrees not to issue invoices hereunder until items or milestones have met Acceptance criteria. Charges for Solutions, products/Solution components, or Services accepted more than ninety (90) days prior to receipt of a valid invoice may not be paid. Should Supplier repeatedly over bill Authorized User, Authorized User may assess a one percent (1%) charge for the amount over-billed for each month that such over-billing continues.

In the event any Deliverable is shipped without the applicable Documentation, payment shall not be due until the required Documentation is provided.

If there are any disputed items, an Authorized User shall pay all undisputed charges and promptly notify Supplier in writing of any disputed amount. Supplier shall thereupon review its records, and, if it does not concur with the Authorized User, provide the Authorized User with documentation to support the charge. If such charges remain in dispute, such dispute shall be resolved in accordance with the Dispute Resolution section of this Contract. In the absence of the Supplier's written evidence identifying the merit of the disputed amounts, Authorized User may not pay the disputed amounts and may consider the matter concerning the specific identified amounts closed. All payment terms are net thirty (30) days after Acceptance.

13. REPORTING

Supplier is required to submit to VITA the following monthly reports:

Report of Sales; and

Small Business Subcontracting Report

These reports must be submitted using the instructions found at the following URL: http://www.vita.virginia.gov/scm/default.aspx?id=97

Failure to comply with all reporting requirements may result in default of the Contract.

Suppliers are encouraged to review the site periodically for updates on Supplier reporting.

14. STEERING COMMITTEE

In order to facilitate mutually beneficial contractual relationships with suppliers, VITA has procedures for establishing a steering committee ("Steering Committee"), consisting of senior management personnel, including personnel involved in the contractual relationship, from VITA and Supplier.

Roles of the Steering Committee include but are not be limited to a) identifying potential issues which may arise during the performance of a contract, b) discussing and assigning roles and responsibilities, c) establishing methods for quickly resolving potential disputes, d) setting rules for communication and decision making, e) monitoring and measuring the business relationship between the parties, and f) acting as a final decision board for escalated problems.

A meeting of the Steering Committee is intended to be a forum for brainstorming and sharing ideas, emphasizing respect, cooperation, and access, with the end goal of developing relationships to avoid conflict. A facilitator may, but is not required to, conduct a meeting of the Steering Committee.

A Steering Committee for this Contract will be formed at VITA's option. Meetings may be held at any time during the Contract term, should VITA, at its sole discretion, determine that a meeting(s) would be beneficial to the contractual relationship, and Supplier agrees to participate in such meeting(s). In addition, Supplier may at any time submit a written request to VITA for a meeting of the Steering Committee, which VITA will not unreasonably deny.

Supplier shall ensure the availability of the appropriate personnel to meet with the VITA contract management team. Additional Steering Committee meetings involving representatives from VITA, the Supplier, and an Authorized User may be required prior to or during performance on any specific SOW issued pursuant to this Contract.

15. AUTHORIZED USER SELF-SUFFICIENCY

Prior to or at any time during Supplier's performance of an order issued, or which may be issued, pursuant to this Contract, an Authorized User may require that Supplier provide to Authorized User a detailed plan to develop Authorized User self-sufficiency and to transition operation and management of a Solution to Authorized User or its Agent, which Agent may be VITA or an agent of VITA or a third party provider under contract with Authorized User. At Authorized User's request and pursuant to an order for Supplier's Services issued hereunder, Supplier shall provide all assistance reasonably required by Authorized User to develop self-sufficiency in operating and managing such Authorized User's Solution. During and/or after the transition period, Authorized User may, at its sole discretion, elect to order or continue Maintenance Services from Supplier for any of the Software or hardware components of the Solution.

16. ESCROW AGREEMENT

Supplier shall maintain copies of all Software source code and related technical and user Documentation, in English, in an escrow account, and shall maintain with escrow agent the executed agreement attached hereto as Exhibit C (Escrow Agreement). VITA acknowledges that, prior to the Effective Date of this Contract, Supplier delivered to VITA and VITA received a copy of the executed Escrow Agreement naming the Commonwealth of Virginia as a third party beneficiary. VITA has reviewed Escrow Agreement to ensure that such Escrow Agreement does not impose upon the Commonwealth any requirements other than administrative responsibilities necessary for the operation of the Escrow Agreement. If events give rise to a need for the escrow agent to release escrowed materials to the Commonwealth, the Commonwealth's sole responsibility shall be to request the release of such materials from the escrow agent. Supplier agrees to notify VITA in writing not less than thirty (30) calendar days prior to termination or any modification of Escrow Agreement. Supplier warrants that the information and materials to be kept in escrow in a media safe environment for the benefit of the Commonwealth are specifically identified and listed in Attachment A to the Escrow Agreement and include the most current version used by all Authorized Users of:

ii. the source code for the Software,

iii. all Documentation related thereto as well as all necessary and available information, proprietary information in English, and

iv. technical Documentation in English which shall enable VITA, any Authorized User, or an Agent of VITA or any Authorized User to create, maintain and/or enhance the Software without the aid of Supplier or any other person or reference to any other materials, maintenance tools (test programs and program specifications), or proprietary or third party system utilities (compiler and assembler descriptions); descriptions of the system/program generation; and descriptions of any Supplier tools required to enable VITA and all Authorized Users to continue to use the Software.

Supplier warrants that the Escrow Agreement provides for, among other items, the release of the list of items on Attachment A of the Escrow Agreement upon the happening of certain events, including, but not limited to, Supplier's failure to carry out its support and maintenance obligations imposed by this Contract for a period of sixty (60) days, Supplier's breach or default under this Contract, Supplier's bankruptcy, Supplier's failure to continue to do business in the ordinary course. Supplier agrees to pay all expenses associated with establishing and maintaining the escrow account and the contents mentioned above.

Subject to the information and materials listed on Attachment A of the Escrow Agreement being released to the Commonwealth pursuant to the terms of the Escrow Agreement, which is an agreement supplementary hereto, Supplier hereby grants to the Commonwealth a royalty-free, perpetual, irrevocable license, that permits disclosure to a third party support-vendor of a complete and accurate copy of then-current source code for the Software licensed hereunder, along with all related documentation.

Any Authorized User which is not a state agency, board, commission, or other quasi-political entity of the Commonwealth of Virginia or other body referenced in Title 2.2 of the Code of Virginia may require Supplier to execute an additional escrow agreement subject to the same requirements and binding Supplier to the same obligations as described above but naming such Authorized User as the beneficiary of the escrow agreement. Subject to the information and materials listed in such escrow agreement being released to such Authorized User, Supplier hereby grants to such Authorized User a royalty-free, perpetual, irrevocable license, that permits disclosure to a third party support-vendor of a complete and accurate copy of then-current source code for the Software licensed to such Authorized User, along with all related documentation.

Supplier has deposited a copy of the source code of the CA Software with Iron Mountain Intellectual Property Management, Inc., 2100 Norcross Parkway, Suite 150, Norcross, Georgia, 30071, USA, Attn: Client Services. Such source code will be updated with each new release of the CA Software which will also be deposited with the escrow agent. Such copies of the source code will be held in escrow and in the event of a final adjudication of CA as bankrupt, Customer will, upon payment of the duplication cost and other handling charges of the escrow agent, be entitled to obtain a copy of such source code. Customer will, however, only use such copy of the source code internally to support the CA Software.

17. RESERVED

18. CONFIDENTIALITY

A. Treatment and Protection

Each Party shall (i) hold in strict confidence all Confidential Information of any other Party, (ii) use the Confidential Information solely to perform or to exercise its rights under this Contract, and (iii) not transfer, display, convey or otherwise disclose or make available all or any part of such Confidential Information to any third-party. However, an Authorized User may disclose the Confidential Information as delivered by Supplier to subcontractors, contractors or agents of such Authorized User that are bound by non-disclosure contracts with such Authorized User. Each Party shall take the same measures to protect against the disclosure or use of the Confidential Information as it takes to protect its own proprietary or confidential information (but in no event shall such measures be less than reasonable care).

B. Exclusions

The term “Confidential Information” shall not include information that is:

i). in the public domain through no fault of the receiving Party or of any other person or entity that is similarly contractually or otherwise obligated;

ii). obtained independently from a third-party without an obligation of confidentiality to the disclosing Party and without breach of this Contract;

iii). developed independently by the receiving Party without reference to the Confidential Information of the other Party; or

iv). required to be disclosed under The Virginia Freedom of Information Act (§§2.2-3700 et seq. of the Code of Virginia) or similar laws or pursuant to a court order.

C. Return or Destruction

Upon the termination or expiration of this Contract or upon the earlier request of the disclosing Authorized User, Supplier shall (i) at its own expense, (a) promptly return to the disclosing Authorized User all tangible Confidential Information (and all copies thereof except the record required by law) of the disclosing Authorized User, or (b) upon written request from the disclosing Authorized User, destroy such Confidential Information and provide the disclosing Authorized User with written certification of such destruction, and (ii) cease all further use of the Authorized User’s Confidential Information, whether in tangible or intangible form.

VITA or the Authorized User shall retain and dispose of Supplier’s Confidential Information in accordance with the Commonwealth of Virginia’s records retention policies or, if Authorized User is not subject to such policies, in accordance with such Authorized User’s own records retention policies.

D. Confidentiality Statement

All Supplier personnel, contractors, agents, and subcontractors performing Services pursuant to this Contract shall be required to sign a confidentiality statement or non-disclosure agreement. Any violation of such statement or agreement shall be shall be deemed a breach of this Contract and may result in termination of the Contract or any order or SOW issued hereunder.

19. INDEMNIFICATION AND LIABILITY

A. Indemnification

Supplier will indemnify, defend and/or, at its option, settle/pay any third party claims that Authorized User’s use of the specific CA Offering licensed or purchased by Authorized User under this

Agreement infringes any valid US patent or copyright within the jurisdictions where Authorized User is authorized to use the CA Offering at the time of delivery. Supplier may, at its option and expense: (i) procure for Authorized User the right to continue to use the CA Offering; (ii) repair, modify or replace the CA Offering so that it is no longer infringing; or (iii) provide a pro-rated refund of the fees paid for the CA Offering which gave rise to the indemnity calculated against the remainder of the Term from the date it is established that Supplier is notified of the third Party claim. If the CA Offering is Supplier software, and is licensed on a perpetual basis, an amortization schedule of three (3) years shall be used for the basis of the refund calculation.

Supplier shall have no liability: (i) in the event the allegation of infringement is a result of a modification of the CA Offering except a modification by Supplier, (ii) if the CA Offering is not being used in accordance with Supplier's specifications, related documentation and guidelines, (iii) if the alleged infringement would be avoided or otherwise eliminated by the use of a Supplier published update or patch, (iv) if alleged infringement is solely the result of use of the CA Offerings in combination with any third party product not provided, authorized or specifically recommended by CA in the applicable CA Documentation, Exhibit I, or (v) if the applicable fees due, via Acceptance for the specific SOW have not been paid. The indemnifications contained herein shall not apply and SUPPLIER shall have no liability in relation to any CA Offering produced by SUPPLIER at the specific direction of Authorized User. THE FOREGOING PROVISIONS STATE THE ENTIRE LIABILITY AND OBLIGATIONS OF SUPPLIER REGARDING CLAIMS OF INFRINGEMENT, AND THE EXCLUSIVE REMEDY AVAILABLE TO AUTHORIZED USER WITH RESPECT TO ANY ACTUAL OR ALLEGED INFRINGEMENT OR MISAPPROPRIATION OF ANY INTELLECTUAL PROPERTY OR OTHER PROPRIETARY RIGHTS.

The Supplier shall indemnify the Commonwealth against all damages, fees, (including reasonable attorney's fees) fines, judgments, costs and expenses finally awarded as a result of a third Party action alleging damage to tangible property, a bodily injury or death, which arises from the provision of services under the Agreement, provided that such liabilities are the proximate result of gross negligence or intentional tortious conduct on the part of Supplier.

The above indemnities are contingent upon: (i) Authorized User providing prompt notice of any claim of infringement and assistance in the defense thereof, (ii) Supplier's right to control the defense or settlement of any such claim, provided that the settlement does not require a payment or admission of liability on the part of Customer, and (iii) Authorized User not taking any actions or failing to take actions that hinder the defense or settlement process as reasonably directed by Supplier. Notwithstanding the precedeing sentence, no legal counsel shall be selected for and no settlement shall be effective as to the Commonewealth wihtout the approval of the Attorney General for Virginia."

B. Liability

EXCEPT IN THE CASE OF A DEATH, DAMAGE TO TANGIBLE PROPERTY, BREACH OF TITLE, INFRINGEMENT OF SUPPLIER'S INTELLECTUAL PROPERTY RIGHTS OR CONFIDENTIALITY, AND OF THIRD PARTY CLAIMS ARISING UNDER THE INDEMNIFICATION SECTION, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, sUPPLIER SHALL NOT BE LIABLE FOR A) ANY INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES OF ANY NATURE, INCLUDING, BUT NOT NECESSARILY LIMITED TO, LOSS OF PROFIT, DAMAGES RELATING TO MONIES SAVED OR FEES GENERATED AND OR ANY LOSS OF DATA BY USE OF ANY CA OFFERING, REGARDLESS OF WHETHER IT WAS APPRISED OF THE POTENTIAL FOR SUCH DAMAGES; AND B) IN NO EVENT WILL SUPPLIER's LIABILITY EXCEED TWICE THE FEES PAID AND OR OWED FOR THE THEN-CURRENT INITIAL OR RENEWAL TERM FOR WHICH THE AUTHORIZED USER HAS PROCURED THE CA OFFERING OR AS FURTHER DEFINED IN THE CONTRACT.

20. INSURANCE

In addition to the insurance coverage required by law as referenced in the Incorporated Contractual Provisions section of this Contract, Supplier shall carry errors and omissions insurance coverage in the amount of $2,000,000 per occurrence.

21. SECURITY COMPLIANCE

Supplier agrees to comply with all provisions of the then-current Commonwealth of Virginia security procedures, published by the Virginia Information Technologies Agency (VITA) and which may be found at (http://www.vita.virginia.gov/library/default.aspx?id=537#securityPSGs) or a successor URL(s), as are pertinent to Supplier's operation. Supplier further agrees to comply with all provisions of the relevant Authorized User's then-current security procedures as are pertinent to Supplier's operation and which have been supplied to Supplier by such Authorized User. Supplier shall also comply with all applicable federal, state and local laws and regulations. For any individual Authorized User location, security procedures may include but not be limited to: background checks, records verification, photographing, and fingerprinting of Supplier's employees or agents. Supplier may, at any time, be required to execute and complete, for each individual Supplier employee or agent, additional forms which may include non-disclosure agreements to be signed by Supplier's employees or agents acknowledging that all Authorized User information with which such employees and agents come into contact while at the Authorized User site is confidential and proprietary. Any unauthorized release of proprietary or Personal information by the Supplier or an employee or agent of Supplier shall constitute a breach of its obligations under this Section and the Contract.

Supplier shall immediately notify VITA and Authorized User, if applicable, of any Breach of Unencrypted and Unredacted Personal Information, as those terms are defined in Virginia Code 18.2-186.6, and other personal identifying information, such as insurance data or date of birth, provided by VITA or Authorized User to Supplier. Supplier shall provide VITA the opportunity to participate in the investigation of the Breach and to exercise control over reporting the unauthorized disclosure, to the extent permitted by law.

Supplier shall indemnify and defend, the Commonwealth, VITA, the Authorized User, their officers, directors, employees and agents from and against any and all fines, penalties (whether criminal or civil),and judgments, , including reasonable expenses suffered by, accrued against, or charged to or recoverable from the Commonwealth, VITA, the Authorized User, their officers, directors, agents or employees, for direct damages suffered by the Commonwealth as a direct result of Supplier's failure r to perform its obligations pursuant this Section.

22. IMPORT/EXPORT

In addition to compliance by Supplier with all export laws and regulations, VITA requires that any data deemed "restricted" or "sensitive" by either federal or state authorities, must only be collected, developed, analyzed, or otherwise used or obtained by persons or entities working within the boundaries of the United States. Authorized User agrees that Supplier Software, Documentation, and or Confidential Information is subject to export controls of the United States of America and import controls of any other country in which such information may be used. Authorized User agrees to export, re-export or import such information only in compliance with such laws and controls.

23. BANKRUPTCY

If Supplier becomes insolvent, takes any step leading to its cessation as a going concern, fails to pay its debts as they become due, or ceases business operations continuously for longer than fifteen (15) business days, then VITA may immediately terminate this Contract, and an Authorized User may terminate an order, on notice to Supplier unless Supplier immediately gives VITA or such Authorized User adequate assurance of the future performance of this Contract or the applicable order. If bankruptcy proceedings are commenced with respect to Supplier, and if this Contract has not otherwise terminated, then VITA may suspend all further performance of this Contract until Supplier assumes this Contract and provides adequate assurance of performance thereof or rejects this Contract pursuant to Section 365 of the Bankruptcy Code or any similar or successor provision, it being agreed by VITA and Supplier that this is an executory contract. Any such suspension of further performance by VITA or Authorized User pending Supplier's assumption or rejection shall not be a breach of this Contract, and shall not affect the rights of VITA or any Authorized User to pursue or enforce any of its rights under this Contract or otherwise.

24. GENERAL PROVISIONS

A. Relationship Between VITA and Authorized User and Supplier

Supplier has no authority to contract for VITA or any Authorized User or in any way to bind, to commit VITA or any Authorized User to any agreement of any kind, or to assume any liabilities of any nature in the name of or on behalf of VITA or any Authorized User. Under no circumstances shall Supplier, or any of its employees, hold itself out as or be considered an agent or an employee of VITA or any Authorized User, and neither VITA nor any Authorized User shall have any duty to provide or maintain any insurance or other employee benefits on behalf of Supplier or its employees. Supplier represents and warrants that it is an independent contractor for purposes of federal, state and local employment taxes and agrees that neither VITA nor any Authorized User is responsible to collect or withhold any federal, state or local employment taxes, including, but not limited to, income tax withholding and social security contributions, for Supplier. Any and all taxes, interest or penalties, including, but not limited to, any federal, state or local withholding or employment taxes, imposed, assessed or levied as a result of this Contract shall be paid or withheld by Supplier or, if assessed against and paid by VITA or any Authorized User, shall be reimbursed by Supplier upon demand by VITA or such Authorized User.

B. Incorporated Contractual Provisions

The then-current contractual provisions at the following URL are mandatory contractual provisions, required by law or by VITA, and that are hereby incorporated by reference: http://www.vita.virginia.gov/uploadedFiles/SCM/StatutorilyMandatedTsandCs.pdf

The contractual claims provision §2.2-4363 of the Code of Virginia and the required eVA provisions at http://www.vita.virginia.gov/uploadedFiles/SCM/eVATsandCs.pdf are also incorporated by reference.

The then-current contractual provisions at the following URL are required contractual provisions, required by law or by VITA, that apply to all orders placed under this Contract that are partially or wholly funded by the American Recovery and Reinvestment Act of 2009 (ARRA) and are hereby incorporated by reference: http://www.vita.virginia.gov/uploadedFiles/SCM/ARRA_Ts_Cs_Rev3.pdf

The then-current terms and conditions in documents posted to the aforereferenced URLs are subject to change pursuant to action by the legislature of the Commonwealth of Virginia, change in VITA policy, or the adoption of revised eVA business requirements. If a change is made to the terms and conditions, a new effective date will be noted in the document title. Supplier is advised to check the URLs periodically.

C. Compliance with the Federal Lobbying Act

Supplier's signed certification of compliance with 31 USC 1352 (entitled "Limitation on use of appropriated funds to influence certain Federal Contracting and financial transactions") or by the regulations issued from time to time thereunder (together, the "Lobbying Act") is incorporated as Exhibit G hereto.

D. Governing Law

This Contract shall be governed by and construed in accordance with the laws of the Commonwealth of Virginia without regard to that body of law controlling choice of law. Any and all litigation shall be brought in the circuit courts of the Commonwealth of Virginia. The English language version of this Contract prevails when interpreting this Contract. The United Nations Convention on Contracts for the International Sale of Goods and all other laws and international treaties or conventions relating to the sale of goods are expressly disclaimed. UCITA shall apply to this Contract only to the extent required by §59.1-501.15 of the Code of Virginia.

E. Dispute Resolution

In accordance with §2.2-4363 of the Code of Virginia, Contractual claims, whether for money or other relief, shall be submitted in writing to the public body from whom the relief is sought no later than sixty (60) days after final payment; however, written notice of the Supplier's intention to file such claim must be given to such public body at the time of the occurrence or beginning of the work upon which the claim is based. Pendency of claims shall not delay payment of amounts agreed due in the final payment. The relevant public body shall render a final decision in writing within thirty (30) days after its receipt of the Supplier's written claim.

The Supplier may not invoke any available administrative procedure under §2.2-4365 of the Code of Virginia nor institute legal action prior to receipt of the decision of the relevant public body on the claim, unless that public body fails to render its decision within thirty (30) days. The decision of the relevant public body shall be final and conclusive unless the Supplier, within six (6) months of the date of the final decision on the claim, invokes appropriate action under §2.2-4364, Code of Virginia or the administrative procedure authorized by §2.2-4365, Code of Virginia.

Upon request from the public body from whom the relief is sought, Supplier agrees to submit any and all contractual disputes arising from this Contract to such public body's alternative dispute resolution (ADR) procedures, if any. Supplier may invoke such public body's ADR procedures, if any, at any time and concurrently with any other statutory remedies prescribed by the Code of Virginia.

In the event of any breach by a public body, Supplier's remedies shall be limited to claims for damages and Prompt Payment Act interest and, if available and warranted, equitable relief, all such claims to be processed pursuant to this Section. In no event shall Supplier's remedies include the right to terminate any license or support services hereunder.

F. Advertising and Use of Proprietary Marks

Supplier shall not use the name of VITA or any Authorized User or refer to VITA or any Authorized User, directly or indirectly, in any press release or formal advertisement without receiving prior written consent of VITA or such Authorized User. In no event may Supplier use a proprietary mark of VITA or an Authorized User without receiving the prior written consent of VITA or the Authorized User.

G. Notices

Any notice required or permitted to be given under this Contract shall be in writing and shall be deemed to have been sufficiently given if delivered in person, or if deposited in the U.S. mails, postage prepaid, for mailing by registered, certified mail, or overnight courier service addressed to:

i). To VITA and to Supplier, if Supplier is incorporated in the Commonwealth of Virginia, to the addresses shown on the signature page.

ii). To Supplier, if Supplier is incorporated outside the Commonwealth of Virginia, to the Registered Agent registered with the Virginia State Corporation Commission.

Pursuant to Title13.1 of the Code of Virginia, VITA or Supplier may change its address for notice purposes by giving the other notice of such change in accordance with this Section.

Administrative contract renewals, modifications or non-claim related notices are excluded from the above requirement. Such written and/or executed contract administration actions may be processed by the assigned VITA and Supplier points of contact for this Contract and may be given in person, via U.S. mail, courier service or electronically.

H. No Waiver

Any failure to enforce any terms of this Contract shall not constitute a waiver.

I. Assignment

This Contract shall be binding upon and shall inure to the benefit of the permitted successors and assigns of VITA and Supplier. Supplier may not assign, subcontract, delegate or otherwise convey this Contract, or any of its rights and obligations hereunder, to any entity without the prior written consent of VITA, and any such attempted assignment or subcontracting without consent shall be void. VITA may assign this Contract to any entity, so long as the assignee agrees in writing to be bound by the all the terms and conditions of this Contract.

If any law limits the right of VITA or Supplier to prohibit assignment or nonconsensual assignments, the effective date of the assignment shall be thirty (30) days after the Supplier gives VITA prompt written notice of the assignment, signed by authorized representatives of both the Supplier and the assignee. Any payments made prior to receipt of such notification shall not be covered by this assignment.

J. Captions

The captions are for convenience and in no way define, limit or enlarge the scope of this Contract or any of its Sections.

K. Severability

Invalidity of any term of this Contract, in whole or in part, shall not affect the validity of any other term. VITA and Supplier further agree that in the event such provision is an essential part of this Contract, they shall immediately begin negotiations for a suitable replacement provision.

L. Survival

The provisions of this Contract regarding Software License, Rights To Work Product, Warranty, Escrow, Confidentiality, and Liability and Indemnification, and the General Provisions shall survive the expiration or termination of this Contract.

M. Force Majeure

No Party shall be responsible for failure to meet its obligations under this Contract if the failure arises from causes beyond the control and without the fault or negligence of the non-performing Party. If any performance date under this Contract is postponed or extended pursuant to this section for longer than thirty (30) calendar days, VITA, by written notice given during the postponement or extension, may terminate Supplier’s right to render further performance after the effective date of termination without liability for that termination, and in addition an Authorized User may terminate any order affected by such postponement or delay.

N. Remedies

The remedies set forth in this Contract are intended to be cumulative. In addition to any specific remedy, VITA and all Authorized Users reserve any and all other remedies that may be available at law or in equity.

O. Right to Audit

VITA reserves the right to audit those Supplier records that relate to the Solution or any components thereof and Services rendered or the amounts due Supplier for such services under this Contract. VITA's right to audit shall be limited as follows:

Three (3) years from Software delivery or Service performance date;

Performed at Supplier's premises, during normal business hours at mutually agreed upon times; and

Excludes access to Supplier cost information.

In no event shall Supplier have the right to audit, or require to have audited, VITA or any Authorized User.

P. Offers of Employment

During the first twelve (12) months of the Contract, should Supplier hire an employee of any Authorized User who has substantially worked on any project covered by this Contract without prior written consent, the Supplier shall be billed for fifty percent (50%) of the employee’s annual salary in effect at the time of termination.

Q. Contract Administration

Supplier agrees that at all times during the term of this Contract an account executive, at Supplier's senior management level, shall be assigned and available to VITA. Supplier reserves the right to change such account executive upon reasonable advance written notice to VITA.

Customer Data RESERVED.

R. Entire Contract

The following Exhibits, including all subparts thereof, are attached to this Contract and are made a part of this Contract for all purposes:

i Exhibit A	Solution Requirements
ii Exhibit B	Solution Options List; Fees, Service Charges, and Payment Schedule
iii Exhibit C	Escrow Letter
iv. Exhibit D	Statement of Work (SOW) Template
v. Exhibit E	Change Order Template
vi. Exhibit F	Reserved
vii. Exhibit G	Certification Regarding Lobbying
viii Exhibit H	CA Order Form
viii. Exhibit I	CA Documentation Arcot Webfort 7.0 and 3.0 Administrative Guides.

This Contract, its Exhibits, and any prior non-disclosure agreement constitute the entire agreement between VITA and Supplier and supersede any and all previous representations, understandings, discussions or agreements between VITA and Supplier as to the subject matter hereof. Any and all terms and conditions contained in, incorporated into, or referenced by the Supplier's Proposal shall be deemed invalid. The provisions of the Virginia Department of General Services, Division of Purchases and Supply Vendor's Manual shall not apply to this Contract or any order issued hereunder. This Contract may only be amended by an instrument in writing signed by VITA and Supplier. In the event of a conflict, the following order of precedence shall apply: this Contract document, Exhibit A, any individual SOW, Exhibit B.

An Authorized User and Supplier may enter into an ordering agreement pursuant to this Contract. To the extent that such ordering agreement, or any order or SOW issued hereunder, include any terms and conditions inconsistent with the terms and conditions of this Contract, such terms and conditions shall be of no force and effect.

VITA and Supplier each acknowledge that it has had the opportunity to review this Contract and to obtain appropriate legal review if it so chose.

Executed as of the last date set forth below by the undersigned authorized representatives of VITA and Supplier.

Name of Supplier	VITA
By: _______________________________	By: _________________________________
(Signature)	(Signature)
Name: ____________________________	Name: ______________________________
(Print)	(Print)
Title: _____________________________	Title: _______________________________
Date: _____________________________	Date: _______________________________
Address for Notice:	Address for Notice:
_________________________________	_________________________________

Executed as of the last date set forth below by the undersigned authorized representatives of VITA and Supplier.

Name of Supplier

By: ________________

(Signature)

Name: Tina M. Ratcliff

(Print) Director - Contracts

Title: ________________

Date: 1/31/13

Address for Notice:

2291 Wood Oak Dr
Herndon, VA 20171

Attention: ________________

VITA

By: ________________

(Signature)

Name: SAM NIXON

(Print)

Title: CIO

Date: 2/13/13

Address for Notice:

11751 Meadowville Lane
Chester, VA 23836
VITA Supply Chain Management

Attention: Contract Administrator

EXHIBIT A REQUIREMENTS
CONTRACT NUMBER VA-130131-CA
BETWEEN
VIRGINIA INFORMATION TECHNOLOGIES AGENCY
AND
CA, INC.

Exhibit A is hereby incorporated into and made an integral part of Contract Number VA-130131-CA ("Contract") between the Virginia Information Technologies Agency ("VITA" or "Commonwealth" or "State") and CA, INC. ("Supplier").

In the event of any discrepancy between this Exhibit A and Contract No. VA-130131-CA, the provisions of Contract No. VA-130131-CA shall control.

A. General

	Requirements	A	B
1.	Does your solution comply with all current COV ITRM Policies and Standards, as applicable, found at: http://www.vita.virginia.gov/library/default.aspx?id=537. If proposed solution does not, please provide details that specify the Standard/Policy and how Supplier's solution does not comply.	Yes	The proposed solution will comply with all applicable current COV ITRM Policies and Standards.

2	Do your proposed interfaces to Commonwealth systems comply with or have approved exceptions to all applicable Commonwealth Data Standards as found at http://www.vita.virginia.gov/oversight/default.aspx?id=10344 If not, please explain.	Yes	The product is compliant with the standards Commonwealth Data Standards
3.	Does your solution/application/product provide effective, interactive control and use with nonvisual means and provide 508 Compliance in accordance with the following standard regarding IT Accessibility and 508 Compliance: http://www.vita.virginia.gov/uploadedFiles/Library/AccessibilityStandard_GOV103-00_Eff_11-04-05.pdf (Refer to www.section508.gov and www.access-board.gov for further information) If yes, please describe how this functionality is achieved and include a completed Voluntary Product Accessibility Template (VPAT) with your proposal: **(**The VPAT template is located in APPENDIX C of the Accessibility Standard (GOV103-00)). If no, does your solution provide alternate accessibility functionality? Please describe.	No	Attached to our response are VPAT"s for CA AuthMinder and CA RiskMinder. The VPAT's indicate the level of compliance of the administrator screens. Many, but not all methods of interactive control and use with non-visual needs are currently supported in the administrator consoles. All of the end user facing screens will all be customized to match the requirements of the Commonwealth including complete 508 compliance. The VPATs are located in Appendix A 7-VPATs

4.	Does your Solution Include support for the following: Knowledge Based Authentication, Risk Based Authentication, Multi-Factor Authentication, and Adaptive Authentication?	Yes	The proposed solution supports a wide range of authentication methods, including Knowledge Based Authentication, Risk Based Authentication, Multi-Factor Authentication, and Adaptive Authentication. For Multi-Factor Authentication CA AuthMinder supports: ▪ CA ArcotID PKI: CA AuthMinder product utilizes a patented credential called a software smartcard, brand named CA ArcotID PKI, which when combined with ID proofing can serve as a NIST Level 3 Assurance credential. ▪ CA ArcotID OTP: This is a software-based application that runs on user's computer and/or mobile device. The CA ArcotID OTP, when combined with ID proofing, can also serve as a NIST Level 3 Assurance credential. ▪ Basic and/or Forms: CA AuthMinder can support basic and/or forms authentication by calling out to external user stores for validation of credentials and/or user-collected attributes (e.g., Active Directory, LDAP, and ODBC). ▪ Email/SMS OTP: CA AuthMinder can support OTP generation on the server-side with delivery to user via email, SMS, or IVR. The SMS and/or IVR requirement can be satisfied by the Commonwealth of VA's existing relationship(s) or CA can provide the SMS and/or IVR capability thru our third party relationship. ▪ Question and Response: CA AuthMinder can support challenge/response authentication (shared secret). ▪ Third-party OTP: CA AuthMinder can support any legacy third-party OTP tokens that support OATH, CAP, or DPA standard algorithms. CA AuthMinder also provides risk-based and adaptive authentication capabilities through its integration with CA RiskMinder, which provides built-in risk-based authentication detects fraudulent activity before losses can occur, without affecting legitimate users. The adaptive risk analysis process assesses the fraud potential of every online transaction by examining a range of data collected automatically. As a result, access is granted, denied or can require additional authentication, all in real-time. You can also implement other third-party or custom authentication mechanisms with CA AuthMinder via the following three approaches: 1. Native integration through standards-based integration, (SAML, RADIUS, OpenID, etc.), 2. Callouts to third-party offering integrated with our rich authentication framework. 3. Plug-ins developed by a third-party or CA.

5	Does your Solution have the ability to be scalable? (i.e. purchasing one or more modules at a time or capable of implementing one module at a time and adding users as needed)	Yes	CA AuthMinder and CA RiskMinder can be purchased and deployed as a joint solution, or individually. In addition, both components can be delivered as an “on-premise” solution or as a cloud-based service. Finally, both CA AuthMinder and CA RiskMinder are very scalable; there are no known scalability limitations. The solution is architected to scale horizontally and vertically to match your current architecture design with regard to load balancing, capacity, high availability, disaster recovery, etc. Vertical scaling is achieved through increasing memory, disk, and processors. Horizontal scaling is achieved through additional local or remote servers with load balancers, and provides performance gains, as well as high availability for critical deployments.
6	Does your Solution include specific hardware and sizing requirements needed for your software to be housed at VITA’s data center?	Yes	Please see Appendix A – CA Advanced Authentication Reference Architecture for details.
7	Does your Solution include documentation describing how long your Solution has been on the market?	Yes	Throughout its 13-year history, CA Advanced Authentication has steadfastly focused at the authentication, fraud/risk marketplace. We continue to make significant investments to ensure that our product is state of the art to help our clients with their current and emerging security challenges.

B. Authentication

	Requirements	A	B
1.	Does your Solution natively integrate with the IBM Security (TIM/TAM/TFIM) product suite to offer KBA?	Yes	The CA Technologies solution includes an out-of-the-box adapter for IBM TAM; please refer to Appendix A 5 TAM Integration Guide. This adapter allows IBM TAM to call out to CA AuthMinder for authentication and to CA RiskMinder for risk evaluation analysis. Integration with IBM TIM, is accomplished by leveraging the API and web services interfaces provided in both components. to request KBA. In addition, these interfaces can also be used to “provision” and “de-provision” users into the CA AuthMinder/CA RiskMinder user stores (from IBM TIM). IBM TFIM can also leverage the API and web services interfaces to request KBA. In addition, CA AuthMinder also supports SAML 2.0, so integration can be done via this protocol. In this situation, CA AuthMinder would be the Identity Provider, and when called by IBM TFIM, it could use KBA (or one of the other supported mechanisms) to authenticate the user.
2.	Does your Solution support custom data stores for knowledge-based authentication?	Yes	CA AuthMinder supports custom data stores for knowledge-based authentication. . For example, a person registering a vehicle might be asked the last six digits of the VIN, license expiration date or other unique information, which can be verified against your back-end DMV data repository in order to authenticate.
3.	Does your Solution have configurable parameters to support varying number of questions?	Yes	The proposed solution may be customized through services to allow varying types of questions and can be configured for the types and number of questions required.

	Requirements	A	B
4.	Does your Solution have configurable parameters to support varying types of questions?	Yes	The proposed solution may be customized through services to allow varying the types of questions.
5	Does your Solution provide multiple types of questions (e.g. true/false, multiple choice, etc.)?	Yes	The solution will query the EDM for questions to be asked and can support various types as determined by the Commonwealth, such as T/F, multiple choice, etc. Configuration of multiple types of questions can be implemented as part of our implementation services.
6	Does your Solution support false negative and/or false positive questions?	Yes	The solution will query the EDM for questions to be asked and can support various types as determined by the Commonwealth, such as T/F, multiple choice, etc. Configuration of multiple types of questions can be implemented as part of our implementation services.
7	Does your Solution have configurable output parameters relative to the types and complexity of questions offered?	Yes	The ability to configure the output, i.e. presentation of the questions, relative to the types and complexity of the questions will be included in the customization provided during implementation
8	Does your Solution support weighted questions?	Yes	The proposed solution will support weighted questions to determine a risk score, with the assumption that those weights have been assigned in the EDM. For example, the question “What was the color of your car in 2011?” doesn’t have the same weight as “What was the exact amount of your Commonwealth Tax Return in 2011?
9	Does your Solution support multiple question profiles for different purposes?	Yes	The system can be configured to support multiple question profiles based on your individual business requirements. For example, profile “X” is assigned to users attempting to obtain a level 2 assurance account and credential, and profile “Z” for users attempting to obtain a higher level account.

	Requirements	A	B
10	Does your Solution have the ability to integrate seamlessly with other authentication types such as risk based, adaptive, or multi-factor?	Yes	CA AuthMinder can be easily integrated with external applications and security systems via several mechanisms, including: ▪ API and web services ▪ WAM solution ▪ Open protocols such as RADIUS,SAML, OpenID and OATH ▪ Cloud-based open protocols ▪ First, web portals and other web-based applications can call out to CA AuthMinder via the following API's: ▪ Issuance API: This API can be invoked by the application to forward issuance requests to CA AuthMinder for enrolling new users and for creating and managing credentials. ▪ Authentication API: This API can be invoked by the application to forward authentication requests to CA AuthMinder. It should be noted that each of these API's is also supported via web services. Second, if there are any SSO and/or WAM solutions present, such as IBM Tivoli the WAM solution would be configured to call out to CA AuthMinder for multi-factor and/or step-up authentication. Third, CA AuthMinder integrates with internal systems such as UNIX servers, VPN's (IPSec and SSL), and other network devices via RADIUS. In addition, internal or external applications can also submit SAML assertions to CA AuthMinder, which would act as the Identity Provider. Fourth, CA AuthMinder can work with any hardware tokens that support standard OATH algorithms. The only requirement is that the token seeds need to be loaded to the CA AuthMinder server, and managed from there going forward. Finally, the CA AuthMinder cloud based authentication service, we support industry standard protocols—SAML 2.0 and Web Services. This allows us to integrate with other on-premise and SaaS applications WAM systems, identity proofing systems, and identity management systems from CA Technologies, Google Apps, IBM, Oracle, Salesforce.com, Sun, Novell, etc.
11	Does your Solution's system support business process decisions/business rule execution throughout the whole software solution?	Yes	The customizable risk engine enables you to configure the solution to match your business practices and risk tolerance, allowing you to easily apply your business rules, rather than forcing you to change your operations to fit your security tool. Additionally, you can integrate the solution with any Internet-facing application via an API. This enables you to add real-time fraud detection quickly and easily to existing business processes and applications.
12	Does your Solution support integrated reporting?	Yes	The CA AuthMinder and CA RiskMinder solution provides a reporting module that includes a set of built-in reports. These reports include user/administrator activity, statistical summaries, and detailed case analyses. The reports can be viewed on the screen and/or exported for further analysis. It also includes a built in authorization model that provides fine-grained access control for each report. In addition, audit data is written to a relational database, so any third-party reporting engine or query tool can be used to build standard reports.

	Requirements	A	B
13	Does your Solution have configurable parameters to support different risk profiles for multiple application types?	Yes	CA RiskMinder allows customers to customize and tailor the rules used to generate a risk score, as well as the actions to take when the risk score reaches a specific threshold. First, CA RiskMinder risk analysis rules can be tailored for different applications and/or different devices being used to access those applications. In addition, different policies can be applied to the resulting risk scores for different user communities. CA RiskMinder evaluates all of the configured rules and calculates a risk score for every transaction; the risk score is then mapped to risk advice, based on configured policies. The risk score and advice are returned to the calling business application allowing it to determine the appropriate action. These rules and risk-evaluation configurations are based on policies and user profile data. Therefore, a gold level business partner could have a different policy applied to their risk score compared to a silver level business partner. In addition, within CA RiskMinder, you define each channel as a different “organization” (CA RiskMinder term), and each organization can have its own set of rules and policies. For example, you can maintain one set of rules for mobile devices, one set for desktops, and one set for IVR. Each set of rules could evaluate different data elements (based on what can be collected and forwarded from each channel), as well as different policies for how to deal with suspicious activity. And, as all historic data is stored, CA RiskMinder can also use rules to look at activities from other channels when performing risk analysis. Second, you can add or change rules on the fly when policies change. If your fraud analysts detect a new trend, new or modified rules can be created and deployed immediately to counter this new threat. Third, CA RiskMinder allows customers to create ‘exception’ rules for users/groups that may override an existing transaction pattern. For example, if you establish a rule that prohibits X transactions per day, but have one or two users/groups who routinely exceed this threshold, you could establish an exception rule for these specific users/groups, so that they will not be flagged. Finally, CA RiskMinder allows customers to build their own rules and/or configure callouts to external sources. It should be noted that most customers first utilize the out-of-the-box rules to collect and analyze data to identify other risk elements. Then they adjust the existing rules to meet their requirements. In addition, new risk elements may be identified leading to the creation of custom rules and/or external callouts.
14	Does your Solution have configurable parameters to support number of registered devices?	Yes	CA RiskMinder can store and associate multiple devices to a single user.

	Requirements	A	B
15	Does your Solution support being introduced into transaction process when called from an external source (e.g. from IBM BPM)?	Yes	CA RiskMinder is designed to “score” any transaction at any point during the application session (whether it is before, during, or after authentication), where a transaction can be anything defined by the customer (e.g., access request, purchase, download, etc.). How the risk is scored for each type of transaction is completely configurable, as is the actions to be taken if the score exceeds specific parameters. Consequently, actions take for one type of application may be completely different for another application. In terms of integration, CA RiskMinder provides Java API and Web Service calls to enable applications to call out to score the risk for a specific transaction.
16	Does your Solution's software comply with the NIST standards for risk based authentication?	Yes	The proposed solution provides the ArcotID PKI credential which complies with NIST Special Publication 800-63-1 up to and including level 3 requirements. When used in conjunction with an appropriate Identity Proofing process, such as leveraging data the Commonwealth has in the DMV databases, this credential will yield a level 2 or level 3 assurance compliant account and credential.
17	Does your Solution's risk and control information include the ability to be documented and tested?	Yes	CA RiskMinder examines a wide range of data it collects automatically about each login or transaction. The self-regulating scoring engine produces a risk score derived from analytics and rules. You can build rules that are specific to your policies and environment and combine rules based on a wide range of transaction and session criteria. You can add or change rules on the fly when policies change. The rules engine consists of rules that can be combined into different rule sets for different transaction types and user groups. The risk evaluation leads to a result for each rule. The combined value of the rules analysis results in a risk score which can be used to override the score from the scoring engine. This allows you to immediately block known fraudulent actions that may not yet be known to the model in the scoring engine. It also allows organizations to make exceptions for users that may override an existing transaction pattern, such as a person traveling in a country that is not part of their established user profile. Administrators can add new rules or configure existing rules to work off revised parameter values. It should be note that most customers utilize the out-of-the-box rules and use CA RiskMinder to then analyze the collected data to identify other risk elements. At that point, existing rules can be adjusted to meet that customer’s experience. Additionally, new risk elements may be identified leading to the creation of new rules to mitigate the newly identified risk. Risk / Fraud departments are able to use CA RiskMinder to craft rules to mitigate transaction risks that they are usually well aware of, but have not had the tools available bring to bear on the problem.

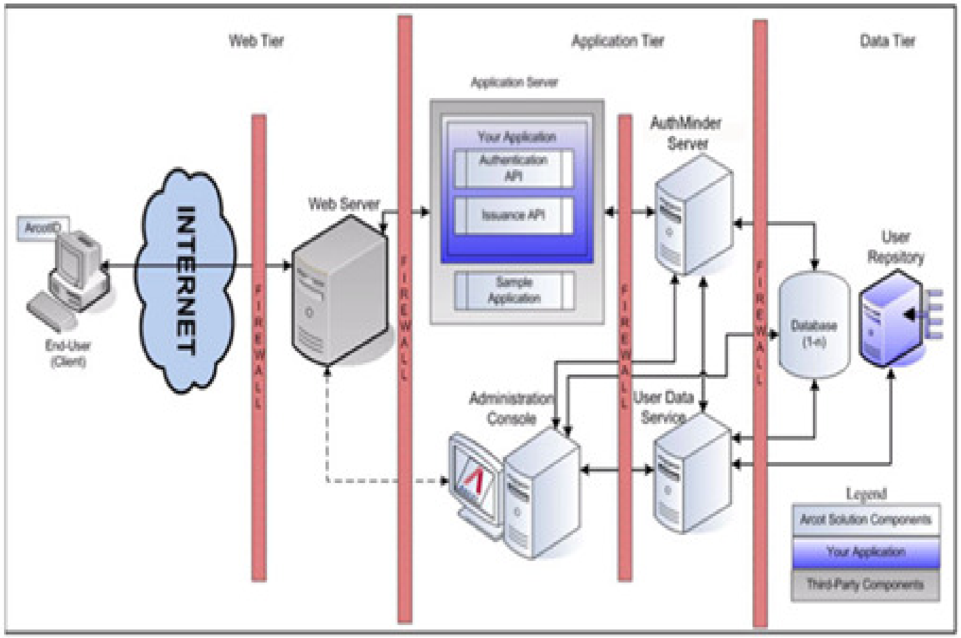
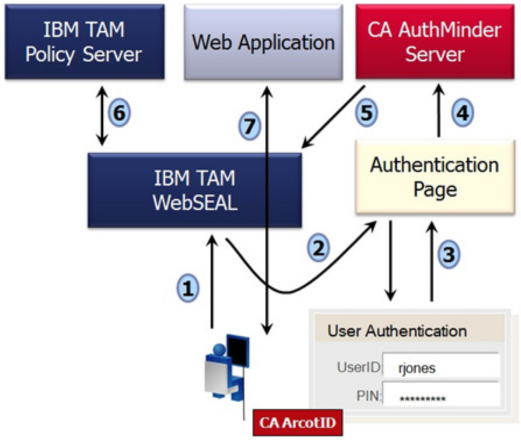
	Requirements	A	B
18	Does your Solution's incidents and events include the ability to be tracked and monitored?	Yes	CA RiskMinder provides an audit trail that annotates each risk analysis and recommended action and has a powerful reporting module that includes a set of built-in reports. These reports include statistical summaries and detailed case analyses. The reports can be viewed on the screen and exported for further analysis. The reporting module runs in an offline database in a data warehouse configuration minimizing impact on the risk assessment system. It also includes a built in authorization model that provides fine-grained access control for each report. In addition, it should be noted that CA RiskMinder provides a web-based interface that can be used to manage high risk transactions (cases). The case management feature provides your administrators and fraud analysts with a single unified view of the data related to cases. This enables them to analyze the data more efficiently and take faster, better-informed decisions towards resolving the cases. Analysts can also constantly track the status and progress of their cases and maintain complete case histories with instant access to all related information. In terms of monitoring, within the Administration Console, CA RiskMinder provides a “statistic page”, which enables an administrator to monitor the connectivity status and details for CA RiskMinder database, UDS, and the transaction statistics for each server instance. By using these statistics, you can tweak your various configuration parameters for better performance.
19	Does your Solution use both historical and contextual information to determine intervention?	Yes	CA RiskMinder will store all contextual data for a transaction that has been evaluated within milliseconds, and can pull this historical data for any new transaction at the time the risk assessment API is called. Therefore, it can pull any transactional data that it is monitoring into the risk assessment automatically. In addition, CA RiskMinder can also pull in any other transactional data that is being monitored elsewhere via custom callouts. CA RiskMinder can be called any number of times during a “complete” on line transaction to score any specific activity within a larger transaction
20	Does your Solution have a configurable rules engine?	Yes	CA RiskMinder provides a fully configurable rules engine. Please see response to Question 13 above for more details.
21	Does your Solution account for false positives and false negatives?	Yes	CA RiskMinder provides the option to temporarily stop a transaction and initiate one of the following actions if the risk score exceeds a policy threshold: ▪ CSR Review: The transaction is forwarded to the Case Management Console for review/approval from a Customer Service Representative. ▪ Step-Up Authentication: CA RiskMinder could query the user for additional credentials, such as challenge/response questions, or could request second factor credential via CA AuthMinder If forwarded to for CSR Review, the transaction could either be marked “fraud” or “not fraud” by the reviewer. If marked fraud, CA RiskMinder will return a “declined” message to the calling application case, which can then terminate the transaction. If marked not fraud, CA RiskMinder will return an “approved” message to the calling application, which can then process the transaction normally. These statistics are then captures in a “false positives” report, which shows transaction activity by rule annotate with fraud, not fraud, and to be determined. Customers can than act upon this data to modify any rules that keep returning false positives.

	Requirements	A	B
22	Does your Solution have a reporting engine for false positives and false negatives?	Yes	CA RiskMinder provides a series of reports that provide statistics and metrics on the system performance. The Fraud Statistics report displays the overall statistical data for each risk advice that CA RiskMinder generates in the specified time. The Rule Effectiveness report displays historical trends for rule activity. The False Positives report shows the transaction activity by rule annotated with fraud, not fraud, and to be determined.
23	Does your Solution support lexical authentication methods?	Yes	The proposed solution may be customized through services to support lexical authentication methods.
24	Does your Solution support graphical authentication methods?	Yes	The system supports the display of a graphical Personal Assurance Message (PAM). The system will prompt the user to select a picture and / or a text message to assist in site authentication, this information is gathered during enrollment. A library of pictures is not included as part of the solution. Additionally, you can deploy an optional patented Scrambled PIN Pad which scrambles the pattern of keyboard character each time your users log in. This has been developed for the purposes of thwarting spyware and key logger based attacks.
25	Does your Solution support one time password authentication methods?	Yes	CA AuthMinder supports several one time password mechanisms, including: ▪ CA ArcotID OTP: This is a software-based OTP generating application that runs on user’s computer and/or mobile device. The CA ArcotID OTP, when combined with ID proofing, can also serve as a NIST Level 3 Assurance credential. ▪ Email/SMS OTP: CA AuthMinder can support OTP generation on the server-side with delivery to user via email, SMS, or IVR. It should be noted that a third-party product is required for SMS and/or IVR delivery of the OTP. ▪ Third-party OTP: CA AuthMinder can support any legacy third-party OTP tokens that support OATH, CAP, or DPA standard algorithms.
26	Does your Solution support X.509 password authentication methods?	Yes	CA AuthMinder utilizes a patented credential brand named CA ArcotID PKI, which is based on a standard X.509v3 digital certificate with a CA “specific” extension. The CA ArcotID PKI utilizes asymmetric (public key) cryptography as the basis for its authentication method. In addition, since the CA ArcotID PKI is entirely software-based, it is very easy to manage and deploy to external user communities (computers or mobile devices) without making any changes to the user’s existing login experience. Finally, it should be noted that CA AuthMinder also includes a completely internal Certificate Authority that is transparently used in the creation and validation of the CA ArcotID PKI credentials.
27	Does your Solution support other token methods (such as a magnetic stripe card, an RFID token, proximity card, etc.)?	Yes	CA AuthMinder can support smartcard and USB key methods as a container for the CA ArcotID PKI credential; this functionality can be delivered through CA services. These methods require a client side application interface. We can call out to other authentication servers for supporting other types of credentials during migration. We current do not support proximity cards.
28	Does your Solution support out of band authentication?	Yes	CA AuthMinder can support out-of-band authentication via OTP generation on the server-side, which can then be delivered via email, SMS, or IVR.
29	Does your Solution support biological biometric authentication?	Yes	The solution can be easily integrated into biometric offerings from third-party vendors by CA’s professional services team, at an additional services costs. This is out of scope for current services proposal.

	Requirements	A	B
30	Does your Solution support behavioral biometric authentication?	Yes	The solution can be customized to support behavioral biometric authentication, from a provider such as BioSig through the use of API's or web services.
31	Does your Solution support a variety of open and proprietary authentication methods in multiplatform environments?	Yes	Please see the response to Question 4 above for the standard authentication methods supported. In addition, you can also implement other third-party or custom authentication mechanisms with CA AuthMinder via three approaches: Callouts, Plug-ins, or by using Custom API's.
32	Does your Solution support cloud-based authentication services?	Yes	CA AuthMinder and CA RiskMinder can be deployed either internally (on-premise) or externally to cloud services (hosted/SaaS). For customers that want to deploy the solutions internally, CA Services can provide architects and/or consultants to help with the installation, configuration, integration, and rollout of the solution. For customers that want a hosted/SaaS-based solution, CA Technologies is the proven leader. Since 2000, CA Technologies has offered cloud-based authentication services and currently serves over 150 million users and 13,000 financial institutions from its SAS 70 Type II audited, PCI DSS-compliant data centers.
33	Does your Solution support web fraud detection capabilities (adaptive authentication, risk based authentication, etc.)?	Yes	CA RiskMinder is an online real-time, rules-based, risk assessment engine. It evaluates "risk" of each transaction and assigns a score for each "risk evaluation" request, returns ▪ Risk Score – a number between 0 (low) and 100 (high) ▪ Risk Action – a string that recommends an action ALLOW, INCR_AUTH, ALERT, DENY ▪ Annotation – details from the risk evaluation CA RiskMinder assesses risk across three categories of behavior: User, Device and IP Geo-location. CA RiskMinder associates users with devices as well as IP geo-location. For analyzing risk, each of these are taken into account relative to each other to identify risk situations whether CA RiskMinder is called to analyze the risk at authentication or in conjunction with transaction risk within an application after authentication. Using statistical techniques, such as Bayesian modeling, to compare each transaction against a scoring formula. CA RiskMinder periodically updates the formula based on recent fraud and transaction data. The out-of-the-box rules are based on CA's decade plus experience with millions of transactions and related authentications to identify risky authentication transaction behavior. Each rule may be modified to suit your preference and indeed additional custom rules may be added to fit exactly your policy or experiential concerns. ▪ Additionally, CA RiskMinder can also be used to monitor post-authentication transactions with rule sets specifically tuned to each transaction type to score the risk profile of any transaction in real-time.

C Technical Architecture

	Requirements	A	B
1	Does your Solution include a description of the architecture model that best describes your system?	Yes	Please see Appendix A.5 TAM Integration Guide for details
2	Does your Solution include a list of the database systems your application supports? If yes, please list all platforms, versions, etc.	Yes	Please see Appendix A 2: CA Advanced Authentication – Server Component Support Matrix
3	Does your Solution include a list of the server platforms your application supports?	Yes	Please see Appendix A 2: CA Advanced Authentication – Server Component Support Matrix
4	Does your Solution include a list of the languages that were used to build your application?	Yes	Please see Appendix A Table 2: CA Advanced Authentication – Server Component Support Matrix.
5	Does your Solution include a list of the web servers your application supports?	Yes	Please see Appendix A 2: CA Advanced Authentication – Server Component Support Matrix for a list of hardware these webservers run on.
6	Does your Solution include a list of the desktop platforms your application supports?	Yes	Please see Appendix A – Table 1: CA AuthMinder CA ArcotID PKI Client Compliance Matrix.
7	Does your Solution include a list of the web browsers that are certified for your application?	Yes	CA AuthMinder and CA RiskMinder support the following browsers: Apple Safari, Microsoft Internet Explorer, Mozilla Firefox and Google Chrome.
8	Does your Solution require any additional browser components for full functionality?	No	The proposed solution does not require any additional browser components to function.
9	Does your Solution include a list of the email programs that are supported by your Solution?	Yes	Any commercially available mail server that supports the Simple Mail Transfer Protocol (SMTP) can serve email messaging. Users may use the email client of their choosing.

10	Does your Solution include a diagram(s) that illustrates your proposed architecture of your Solution? If yes, please include all environments that will be required including test, development, UAT, etc …	Yes	This is a typical deployment architecture for our solution. Scalability is achieved through multiple servers and load balancers. Similar architectures are used in Development, Test, UAT and production environments as required.  Web Tier Application Tier Data Tier Application Server Your Application Authentication API Issuance API Sample Application AuthMinder Server User Repository Database (1-n) ArcotID End-User (Client) INTERNET FIREWALL FIREWALL FIREWALL FIREWALL Web Server Administration Console User Data Service Legend Arcot Solution Components Your Application Third-Party Components  IBM TAM Policy Server Web Application CA AuthMinder Server IBM TAM WebSEAL Authentication Page 1 2 3 4 5 6 7 User Authentication UserID rjones PIN CA ArcotID 1. User attempts to access a protected web application 2. WebSEAL redirects user to a login page that includes a "challenge" 3. User enters UserID/PIN – CA ArcotID on user's local system 4. CA AuthMinder server validates "signed challenge" from CA ArcotID 5. CA AuthMinder server passes user "credential" to IBM TAM WebSEAL that identifies user 6. TAM Policy Server decides if user is allowed access 7. TAM WebSEAL grants access to authorized pages

11	Does your Solution include white papers, architecture diagrams, data flows, or other supporting documentation?	Yes	CA Technologies offers a comprehensive library of white papers, architecture diagrams, data flows, sizing guides, deployment guides, installation guides, administration guides, implementation guides, support matrix guides and other documentation. Documentation is available to download on the CA Support website and/or distributed as requested or required.
12	Does your Solution include a description of your preferred combination of hardware, operating systems, web servers (if applicable), and client software used by the majority of your clients?	Yes	We support a number of configuration options that are detailed in Appendix A. We do not have records of the various combinations our customers have chosen.
13	Does your Solution include an architecture diagram of the preferred architectural design, including information on the recommended operating system and web server version combinations for each physical server?	Yes	The solution is supported on Windows, X86 Solaris and RHEL. Choice of operating systems is typically made by the customer based on their knowledge and requirements. Please see our support matrix for combination of platforms, app servers and databases that are supported. The logical architecture for our solution is illustrated above, in our response to question 10, in this section. In addition, our solution integrates with the IBM TAM solution, as shown below:

D Database

	Requirements	A	B
1	Does your Solution include a database platform that is used for the application instances?	No	CA AUTHMINDER AND CA RISKMINDER MAKE USE OF EXISTING DATABASES, A LIST OF SUPPORTED DATABASES IS INCLUDED IN APPENDIX A - TABLE 4: CA ADVANCED AUTHENTICATION – REPOSITORY SUPPORT MATRIX
2	Does your Solution include a description of the database reporting tools used in your Solution?	Yes	CA AuthMinder and CA RiskMinder provides a reporting module that includes a set of built-in reports. These reports include user/administrator activity, statistical summaries, and detailed case analyses. The reports can be viewed on the screen and/or exported for further analysis. The reporting module runs in an offline database in a data warehouse configuration minimizing impact on the risk assessment system. It also includes a built in authorization model that provides fine-grained access control for each report. In addition, audit data is written to a relational database, so any third-party reporting engine or query tool can be used to build standard reports.
3	Does your Solution include an encrypted database? If yes, please explain how it is encrypted?	No	The CA Advanced Authentication solutions leverage an external relational database.
4	Does your Solution include a description of the technology used for your Solution's repository?	Yes	CA AuthMinder and CA RiskMinder each require its own user store (Oracle and MS SQL databases are supported). Please see Appendix A 4 Repository Support Matrix for more details.

5	Does your Solution include a description of the database that is used for development and test environments?	Yes	CA AuthMinder and CA RiskMinder require its own data repository, (Oracle and MS SQL databases are supported). Please see Appendix A 4 Repository Support Matrix for more details.
6	Does your Solution allow the database to be accessible for use by other applications?	Yes	We only require name space in an existing database, not a dedicated database. Access to most of the data stored in our repository can be accessed via an API
7	Does your Solution allow easy access to the database directly? (Ex. No proprietary encryption, odd or cryptic table / field names, etc.)	Yes	Access to most of the data stored in our repository can be accessed via an API.
8	Does your Solution include tools to help size the system database?	Yes	The solution includes sizing guides to assist is sizing the database.
9	Does your Solution include items for install and sizing scripts for the system database objects?	Yes	The solution includes database scripts to set correct installation and sizing parameters.
10	Does your Solution's application depend on a specified schema owner or user names/passwords to the database?	Yes	The database owner is defined during the initial installation. The database vendor's "best practices" policies around individual database security and performance should be followed.
11	Does your Solution's schema owner need DBA access for the application to function?	Yes	The schema owner is created during the initial installation and only this owner is granted access to the schema.
12	Does your Solution include any system database functions that require DBA access to be performed?	Yes	Standard Installation requires users and permissions to be created.
13	Does your Solution's application require a specific operating system for the database server?	No	The CA Advanced Authentication solutions use standard protocols to communicate with the databases, so the underlying OS running the database is not applicable.
14	Does your Solution include any messaging software that your system uses to connect to the database?	No	The CA Advanced Authentication solutions leverage JDBC device drivers.
15	Expanding on the question above, does your Solution's connections stay connected at all times, or are they transaction-based?	Yes	The solutions are connected all the time and takes advantage of connection pooling for additional performance enhancements.

E Performance

	Requirements	A	B
1	Does your Solution have a maximum number of named users, logged-on users, and concurrent users that it will accommodate? If yes, please explain and include documentation regarding your largest implementations.	Yes	There is no theoretical limit to the number of users that the system can accommodate.

2	Does your Solution have a maximum number of concurrent transactions that it will support?	Yes	There is no theoretical limit to the number of users that the system can accommodate. The solution should be sized to meet the peak number of transactions per hour. Our services team can help size the implementation for expected performance.
3	Does your Solution include a list detailing the hardware system requirements for a user base of 1.5M and 3M?	Yes	CA does provide some sizing guidelines (see Appendix A); however, it should be noted that server sizing is more dependent upon the number of transactions per minute vs. the number of named users, A final complete recommendation will be providing during the planning phase of the deployment.
4	Does your Solution include descriptions of any documented stress testing methods /results?	No	Due to the ability of the solution to scale horizontally via load balancers, we do not have any documented stress test methods.
5	Does your Solution include a description of the average amount of data transmitted per request?	No	For authentication requests there is a challenge response dialog that occurs between the client machine and the server. This is small in nature and does not affect performance in any way.

F Product Licensing

	Requirements	A	B
1	Does your Solution require any third-party software packages?	Yes	You will need to provide the operating systems, database(s), Web Servers and App Servers required for implementation, supported platforms are listed in Appendix A.
2	Expanding on the question above, if your Solution requires third-party software packages, does your Solution include them?	No	All third-party software licenses (e.g., app server, database server, OS, etc.) must be purchased separately. If the Commonwealth would like to use the integrated SMS/IVR delivery capability of the solution, that is separately priced per transaction. Alternatively the Commonwealth may leverage existing SMS services providers, which can be integrated into the solution by CA Services for an additional fee.
3	Does your Solution require any separate licenses?	No	Not for the CA products provided to complete this solution.
4	Does your Solution include a strategy for providing coordination of support for third-party packages?	Yes	If support identifies an issue with third-party products an information bulletin would be sent detailing the steps required for patching or upgrading.
5	Does your product have any industry certifications (e.g. FICAM, etc.)?	Yes	Our hosted (SaaS) solution goes through a complete annual PCI Audit, annual SAS 70 Type II audit, and is pending FISMA/DIACAP audit completion. Our ArcotID PKI credential has FIPS 140-2 certification.
6	Is your product licensed by an enterprise approach?	Yeses	In an effort to align to this RFP, our pricing is based on 3.5 million users for both AuthMinder and RiskMinder. If we are chosen as a finalist, CA would welcome the opportunity to discuss an enterprise licensing model for the Commonwealth of VA.

G Integration

	Requirements	A	B
1	Does your Solution require any third-party integration tools? (i.e., messaging, EAI)	No	No third party tools are required.
2	Does your Solution have any existing known hardware/software incompatibilities?	No	The CA solutions have no known incompatibilities when running on the certified platforms listed in Appendix A.
3	Does your Solution include an API for accessing the system and data?	Yes	Web portals and other web-based applications can call in to CA AuthMinder and CA RiskMinder. The solution also provides API's to integration to customers applications and processes.
4	Does your Solution include data import and export formats? If yes, please describe the formats that are supported by your Solution.	Yes	Data can be exported to a CSV file format for further reporting, analysis and integration. Data can be imported via our APIs. The file format is typically a text flat file or database table.
5	Does your Solution include versions of the operating system that are certified for running the application?	No	CA does not provide OS licenses.
6	Does your Solution include supported versions of the operating system? If yes, please list the supported versions.	No	These must be licensed separately. We operate on Windows, Solaris and Linux. Details can be found within Appendix A - Table 2: CA Advanced Authentication – Server Component Support Matrix.
7	Does your solution natively integrate with the IBM Security toolset TIM/TAM/TFIM?	Yes	Please see response to Question 1 in Section B – Authentication for details.

H System Management

	Requirements	A	B

1	Does your Solution include any troubleshooting (debugging) tools?	Yes	The CA Advanced Authentication solutions provide several log files that enable you to monitor activity and performance of the server and to effectively manage the communication between CA AuthMinder and CA RiskMinder Servers and your application, as well as troubleshoot any problems that have occurred. The log files can be categorized as: ▪ Startup Log File: When you start the AuthMinder or RiskMinder Servers, they record all start-up (or boot) actions in this log file. The information in this file is very useful in identifying the source of the problems if the service does not start up. ▪ Transaction Log Files: The transaction logs consist of the following types: ▪ CA AuthMinder Server Log – this is record of all requests processed by the server. ▪ CA AuthMinder Statistics Log File – this is used for logging statistics ▪ CA RiskMinder Server Log – this is record of all requests processed by the server. ▪ CA RiskMinder Statistics Log File – this is used for logging statistics UDS Log File: All User Data Service (UDS) information and actions are recorded in this log file. This information includes: – UDS database connectivity information – UDS database configuration information – UDS instance information and the actions performed by this instance The information in this file is very useful in identifying the source of the problems if the Administration Console could not connect to the UDS instance Administration Console Log File: This file contains the details of all actions and processed requests that were submitted via the Administration Console.
2	Does your Solution require administrative rights for client or service accounts?	No	The solution is accessed via secure web pages. Administrative rights are delegated down from the system super user account.
3	Does your Solution's console access (login/logout) affect the application?		The solutions console access may affect the application, depending on the access rights delegated to a subordinate administrator. All change events are logged for auditing purposes.
4	Does your Solution have any support restrictions for system patching?	No	CA does recommend that CA AuthMinder& CA RiskMinder servers be upgraded via a rolling upgrade process, such that each server is upgraded separately, thus negating the need for a service outage. In addition, new releases provide notes that specify the steps to apply a new release. In most cases, the installation wizard handles the release update; however, in some cases, scripts are provided to ease the upgrade.
5	Does your Solution include a description of the platform that your development team wrote and tested this application with initially?	Yes	The CA AuthMinder and CA RiskMinder solutions were developed on Windows using C++ and Java. We have expanded our support to include Red Hat Linux and Solaris. (Please refer to Appendix A 2 Server Component Support Matrix for a complete list of platforms we support.)

I Security and Access Control

	Requirements	A	B
1	Does your Solution's application require integration with any services for authentication and group membership?	No	All administrative users must authenticate via basic authentication (username/password) provided and implemented by the Administration Console authenticated by AD or via the use of ArcotID PKI CA AuthMinder username/password credentials, before they can access the Administrative Console. Login credentials are stored in the application user store. End users do not access the application directly.

2	Does your Solution include a definition of the user roles, groups and polices required for implementation?	Yes	The Administration Console supports the following types of roles: Users, Default Administrative Roles, and Custom Roles. Each is described in more detail below. **Users** Every end user of your online application system is referred to as a user in Administration Console. This user can either exist in your Lightweight Directory Access Protocol (LDAP) repository or in CA Advanced Authentication database. If the user already exists in your LDAP system, then you need to map the organization LDAP attributes to CA supported attributes. **Default Administrative Roles** The Administration Console is shipped with an out-of-the-box administrator called the Master Administrator who can perform high-level configurations. Other than this, you must assign users to administrative roles to administer the CA Advanced Authentication system or to access business data. The users with administrative privileges are referred to as administrative user. An administrative role typically comprises a set of privileges based on a job function profile and the scope in which these permissions are applicable. The Administration Console supports the following pre-defined administrative roles: ▪ Master Administrator ▪ Global Administrator ▪ Organization Administrator ▪ User Administrator It should be noted that every administrator is also considered a user of the system. **Custom Roles** Finally, a Master Administrator can also create new administrative roles that inherit a subset of privileges from one of the following predefined parent roles: ▪ Global Administrator ▪ Organization Administrator ▪ User Administrator These roles are called custom roles, and are derived by disabling some of the default privileges associated with the parent role. For example if you need to disable the "Organization Creation Privilege" for a GA, then you can create a Custom role by disabling this privilege.
3	Does your Solution's application require integration with any third-party web single sign-on products?	No	The solution does not require integration with third-party web single sign-on products.
4	Does your Solution's application support concurrent authentication methods (i.e. users could authenticate using active directory or internal authentication)?	Yes	The product can be used in combination with other authentication methods. Users are authenticated either via AD or CA AuthMinder credentials as assigned per the user's group.

5	Does your Solution include a description of the security of your application? If yes, please explain how you developed your application with security in mind.	Yes	The CA AuthMinder credentials (CA ArcotID PKI and CA ArcotID OTP) are secured during initial provisioning and subsequent usage. During provisioning process, the key is protected by encrypting the channel between the mobile and the server via SSL. In addition, we "camouflage" the keys in transit with the user's activation key. On the workstation or mobile device, the credentials are protected by our patented Cryptographic Camouflage (US Patent 6,170,058) for protection of sensitive key/seed information We camouflage the private key or “seed value” with the user's password. Camouflaging ensures that a fraudster cannot perform a brute force attack to retrieve the key. The key will only be decrypted after the user has entered their password. Finally, Communication between the workstation/browser and application is usually secured via SSL by the authenticating site. Also, all components within the CA solution such as the administration console, web-services and SDKs can be configured to use SSL for transport security while communicating with the CA AuthMinder and CA RiskMinder servers. It should be noted that the CA AuthMinder server can also leverage an HSM for key protection on the server side. The CA solution is penetration-tested and the code is inspected with code analysis tools for security vulnerabilities. All discovered vulnerabilities are documented and high-risk vulnerabilities are remediated. The CA solution is built such that all sensitive data, including personally identifiable information (PII), passwords, account information etc., are encrypted when in transit over the network (between the web-server and the browser, as well as between the application server and external interfaces, e.g. web-services, databases) and when stored at rest.

<table>
<tr><td>6</td><td>Does your Solution include an explanation of how your application utilizes secure protocols? If yes, please describe the protocols that are supported by your Solution.</td><td>Yes</td><td>Communication between applications and CA Advanced Authentication is conducted via API or web services, and is typically performed behind the firewall. Communications between applications and cloud-based CA Advanced Authentications uses SAML 2.0.
<table>
<tr><th>Protocol</th><th>Default Port Number</th><th>Description</th></tr>
<tr><td>Server Management Web Services</td><td>9743</td><td>This protocol is used for managing CA AuthMinder server. Administration Console and arwfclient clients communicate using this port for server management activities.</td></tr>
<tr><td>Transaction Web Services</td><td>9744</td><td>This protocol is used by the Authentication and the Issuance Web services client to connect to CA AuthMinder Server.</td></tr>
<tr><td>Authentication Native</td><td>9742</td><td>This is a proprietary, binary protocol used by CA AuthMinder for the purpose of authentication. This port is used by the Authentication SDK.</td></tr>
<tr><td>Administration Web Services</td><td>9745</td><td>This protocol is used to create and manage configurations, such as profiles, policies, SAML, and ASSP configurations.</td></tr>
<tr><td>RADIUS</td><td>1812</td><td>This is used to support the Remote Authentication Dial In User Service (RADIUS) protocol. When configured to support RADIUS protocol, CA AuthMinder server acts as a RADIUS server.</td></tr>
<tr><td>ASSP</td><td>9741</td><td>This protocol is used with Adobe® Reader and Adobe® Acrobat® to authenticate user for server-side digital signing of the PDF documents.</td></tr>
<tr><td>Transaction HTTP</td><td>9746</td><td>This protocol is used to transfer the HTTP request packets from the HTTP Client to the CA AuthMinder Server.</td></tr>
</table></td></tr>
<tr><td>7</td><td>Does your Solution include an explanation of the ports and services that are utilized by the application?</td><td>Yes</td><td>Please refer to the table in the question above, 6.</td></tr>
<tr><td>8</td><td>Does your Solution require root or administrator access when running the application?</td><td>No</td><td></td></tr>
<tr><td>9</td><td>Does your Solution's application require any modifications to the operating system when running?</td><td>No</td><td></td></tr>
</table>

10	Does your Solution include an explanation of how access permissions are set and modified?	Yes	The CA AuthMinder and CA RiskMinder solutions fully support role-based access control (RBAC). Internal administrative roles enable you to specify which operations and privileges are assigned to a user or a set of users who share similar responsibilities. When a user is assigned to a specific role, the set of functions called tasks that are associated to that role become available to the user. As a result, administrators can exercise fine-grain control on the tasks assigned to each user in the system. The default administrator roles and how to customize these roles are defined within the product documentation.
11	Does your Solution include a description of the administrator's role?	Yes	The following summarizes the privileges available to the supported four levels of administrators. The column name acronyms used in the table are: ▪ Master Administrator --> MA ▪ Global Administrator --> GA ▪ Organization Administrator--> OA ▪ User Administrator --> UA Please see Appendix A.6 Administrator privileges for more detail
12	Does your Solution allow the administrator to reset a user password?	N/A	The CA AuthMinder solution does not store the user password/PIN, which is used to encrypt / decrypt the CA ArcotID PKI/CA ArcotID OTP key; therefore, we do not provide “password reset/change” capabilities. However, we do provide an out-of-the-box solution for changing or resetting the private key. This is the same activity as if the user has forgotten their password/PIN. However, instead of just changing or resetting their password, we provide a mechanism for the user to request a new key via step-up authentication (OTP via SMS or challenge/response questions). Successful completion of this will trigger a new credential to be generated and downloaded to the respective device. At the same time, the user will be prompted to enter a new password/PIN to encrypt the new key. Therefore, this approach does allow users to change/reset a forgotten password, but it also replaces the previous key at the same time. This capability can also be triggered by an administration.
13	Does your Solution's application allow the administrator to set security rules and password controls?	Yes	Please see Appendix A.6 Administrator privileges for more detail

14	Does your Solution enforce password changes? If yes, can we indicate what the length of time is?	Yes	A Username-Password profile can be used to specify the following attributes related to a password credential: ▪ Password strength: The effectiveness of password, which is determined by the length of the password and number of alphabets, numerals, and special characters in it. ▪ Validity period: The period for which the username-password credential is valid. ▪ Auto-generate password: (The password is generated by the AuthMinder Server.) ▪ Usage count: Number of times the password can be used. ▪ Usage type and password uniqueness: Multiple passwords can be set for a user, which can be the same or unique. ▪ Partial password settings: User is prompted for password characters in different positions. – Minimum Character: Specify the least number of characters that the password can contain. You can set a value between 4 and 64 characters. The default value is 6. – Maximum Characters: Specify the most number of characters that the password can contain. You can set a value between 4 and 64 characters. The default value is 10. – Minimum Alphabetic Characters: Specify the least number of alphabetic characters (a-z and A-Z) that the password can contain. This value must be lesser than or equal to the value specified in Minimum Characters field. – Minimum Numeric Characters: Specify the least number of numeric characters (0 through 9) that the password can contain. You can set a value between 0 and 32 characters. – Minimum Special Characters: Specify the least number of special characters that the password can contain. By default, all the special characters excluding ASCII (0-31) characters are allowed. – Validity Start Date: Set the date from which the issued password credential will be valid. The validity can start from either the date when this credential is created or you can specify a custom date. – Validity End Date: Set the date when the password will expire. You can either specify the duration for the credential's expiration or you can specify a custom date.
15	Does your Solution always transmit and store passwords in a one-way encrypted format?	N/A	CA AuthMinder does not store user passwords within its user stores. The CA ArcotID PKI and/or CA ArcotID OTP application will prompt user to enter their password in order to encrypt/decrypt the private key stored on the client; the password is never transmitted over the wire or stored within the AuthMinder system. In addition, CA AuthMinder can provide its patented Scrambled Pin Pad to protect the password from key loggers.
16	Does your Solution allow passwords to be seen by administrators?	No	The solution is based on a closed PKI system. The password is only known to the end-user. If a user forgets their password, a new token-passphrase will be generated and the old credential is revoked and a new one is issued.

17	Does your Solution include the use of encryption protocol while transferring data?		All connections between the client and CA AuthMinder/CA RiskMinder servers and the servers and any backend data stores are done via SSL secured protocols.
18	Does your Solution include a description of the encryption level used to store data?	Yes	The CA AuthMinder solution is FIPS 140-2 certified (Certificate No. 818) and supports (in FIPS mode), the following FIPS Approved cryptographic algorithms: ▪ Triple-DES: ECB, CBC, OFB (64-bit), CFB (64-bit) – Certificate No. 499 ▪ SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 – Certificate No. 558 ▪ RSA PKCS#1 (sign/verify): Modulus sizes: 1024, 2048, 4096 and SHS: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 – Certificate No. 201 ▪ RSA-PSS (sign/verify). Modulus sizes: 1024, 2048, 4096 and SHS: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 – Certificate No. 201 ▪ HMAC. SHS: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 – Certificate No. 242 ▪ ANSI X9.31 Pseudo-Random Number Generation (PRNG) – Certificate No. 268 In addition, in FIPS mode, the module also supports the following non-FIPS Approved cryptographic algorithms: ▪ RSA encryption and decryption (for key wrapping). The module allows these algorithms in FIPS mode because they meet all requirements described in “Annex D: Approved Key Establishment Techniques for FIPS PUB 140-2.” ▪ RSA PKCS#1 key generation (Modulus sizes: 1024, 2048, and 4096). It should also be noted that in “non-FIPS mode”, the cryptographic module also provides non-FIPS Approved hash algorithms as follows: ▪ MD5 ▪ MD4 ▪ MD2 ▪ RIPEMD-160 The above hash algorithms will only execute when the module is in non-FIPS mode, and only when they are used as the hash algorithm for RSA signing and RSA verification operations.
19	Does your Solution allow end users to have a direct connection to the database? If yes, please explain how the security through this connection is managed.	No	The solution utilizes Java Database Connectivity (JDBC) to connect to the database. The JDBC driver supports the use of SSL JDBC for enhanced security.
20	Does your Solution include any level of encryption to encrypt data in transit?	Yes	All connections between the client and CA AuthMinder/CA RiskMinder servers and any backend data stores are done via SSL secured protocols.
21	Does your Solution include the validation of user input to prevent malicious use of the application?	Yes	During initial creation of an ID, the user is sent an activation code to prevent malicious attempts to gain access to the system by non-authorized users. The activation code can be set to expire after a pre-set time. Users already in the system can be sent an OTP via SMS, email or generated via Smart device. (Phone, tablet, etc.)

22	Does your Solution support disconnected tokens?	Yes	The proposed solution supports disconnected tokens. For out-of-band authentication, our solution provides a secure, software-implemented One-Time-Passcode generator that can be run on smartphones, tablets, thus allowing these to be used as convenient authentication devices. This generator provides support for OATH-compliant token generation. Our solution also works with other 3rd party OATH-compliant tokens.
23	Does your Solution support connected tokens?	Yes	We support ArcotID's stored on a USB thumb drive. This use case requires the installation of our native client or java applet on the users PC.
24	Does your Solution support soft tokens?	Yes	The CA ArcotID PKI is a software-based token. The CA ArcotID PKI is a secure software-implemented container of the private key used in PKI-based 2-factor authentication. Further, for out-of-band authentication, our solution provides CA ArcotID OTP, a software-implemented One-Time-Passcode generator.
25	Does your Solution support one time tokens?	Yes	CA AuthMinder supports several one-time password mechanisms, including: ▪ CA ArcotID OTP: This is a software-based OTP generating application that runs on user's computer and/or mobile device. The ArcotID OTP, when combined with ID proofing, can also serve as a NIST Level 3 Assurance credential. ▪ Email/SMS OTP: CA AuthMinder can support OTP generation on the server-side with delivery to user via email, SMS, or IVR. The SMS and/or IVR requirement can be satisfied by the Commonwealth of VA's existing relationship(s) or CA can provide the SMS and/or IVR capability thru our third party relationship. ▪ Third-party OTP: CA AuthMinder can support any legacy third-party OTP tokens that support OATH, CAP, or DPA algorithms.
26	Does your Solution support out of band communication?	Yes	CA AuthMinder can support out-of-band authentication via OTP generation on the server-side, which can then be delivered via email, SMS, or IVR. It should be noted that a third-party product is required for SMS and/or IVR delivery of the OTP.
27	Does your Solution support device fingerprinting?	Yes	CA RiskMinder can "fingerprint" any device using its patented DeviceDNA technology when the connection is "browser-based". One of the primary risk elements used within the risk analysis is the DeviceDNA data, which is collected via the browser header objects or via Flash and Java Script (all which are browser-based). The DeviceDNA provides a unique identifier for the device and CA RiskMinder can use device identification in calculating the level of risk for a transaction, and device identification can be done at multiple points within the user's session (e.g., at authentication time or during a specific transaction). In addition, CA RiskMinder will store DeviceDNA data within the user's profile, so that it can be used in historical pattern analysis. In terms of supported devices, in the past, we have collected Device DNA data on mobile devices (including tablets), and other non-pc devices if they are using a browser to connect. In terms of applications which use a thick client (such as mobile applications), CA RiskMinder API's could be embedded within the mobile clients, which could collect and forward the device DNA data elements necessary for risk analysis to CA RiskMinder. This data could be passed through the application itself (which would result in a server-side call to CA RiskMinder) or directly by the CA RiskMinder API.

28	Does your Solution support PIV/PIV-I credentials?	No	CA AuthMinder does not natively support PIV/PIV-I credentials, typically these types of credentials are used by internal users, and authentication is handled by a Web Access Management tool such as CA SiteMinder or IBM TAM
29	Does your Solution support biometrics?	Yes	Biometric offerings from third-party vendors can be integrated into the solution by CA Professional Services.
30	Does your Solution support challenge/response capabilities?	Yes	CA AuthMinder supports PKI based challenge/response authentication.
31	Does your Solution integrate with any third party factors? If yes, please explain and list all third party factors	Yes	CA AuthMinder can be integrated with and authenticate OATH third-party One-Time Password (OTP) tokens. Since the OTP algorithms are standards-based, CA AuthMinder can work with any hardware tokens that support the OATH algorithms. The only requirement is that the token seeds need to be loaded to the CA AuthMinder server, and managed from there going forward. This can be accomplished implemented by CA professional Services at an additional cost. Additional third-party factors can be integrated via SAML, RADIUS, OpenID, Challenge-response or Web Service API.
32	Does your Solution support integrated reporting?	Yes	The CA AuthMinder and CA RiskMinder solution provides a reporting module that includes a set of built-in reports. These reports include user/administrator activity, statistical summaries, and detailed case analyses. The reports can be viewed on the screen and/or exported for further analysis. The reporting module runs in an offline database in a data warehouse configuration minimizing impact on the risk assessment system. It also includes a built in authorization model that provides fine-grained access control for each report. In addition, audit data is written to a relational database, so any third-party reporting engine or query tool can be used to build standard reports.

J. Upgrades and Releases

	Requirements	A	B

1	Does your Solution's periodic maintenance include updates and upgrades to the application? If yes, please explain the frequency of the upgrades.	Yes	Historically, CA plans for one major release every 12-18 months. Major releases may contain the following: ▪ Significant new features and functionality ▪ Product architectural updates ▪ Problem fixes/emergency patches accumulated since last release of the software In addition, CA also plans for two minor releases and/or service packs per year. These may contain the following: ▪ Be created to deliver a limited subset of major new functionality to the market. This new functionality may require schema changes and may require customers to migrate their data to utilize the product. ▪ Be used as a mechanism to add platform, directory, and data base support to the base product ▪ Always contain cumulative fixes made since the last release of the product ▪ Include combinations of items above Finally, CA also provides Cumulative Releases. Cumulative releases for key products are prepared and released on a regularly scheduled basis by designated Development team. For example, the goal for most CA products is to have, at most, a monthly release. Cumulative releases are comprised of a relatively small number of accumulated, tested bug fixes. Most fixed bugs contained in Cumulative Releases (CRs) are customer reported P1and P2 escalations that have been resolved. Internally discovered P1 and P2 problems / tested fixes may also be included in a Cumulative Release. Additionally, emergency patches to fix any security vulnerabilities and/or to address severity 1 issues may be released as soon as the patches are available.
2	Does your Solution include a schedule of major releases? If yes, please state when your next major release is due to be scheduled.	Yes	The next release of CA AuthMinder and CA RiskMinder post 6.2 (CA AuthMinder) and post 2.2.6 (CA RiskMinder) and is planned for release in early 2013.
3	Does your Solution include a description of customizations or configurations rolled forward in an upgrade?	Yes	All enhancements are described within the release notes.
4	Does your Solution allow an upgrade or release be skipped?	No	The upgrade process will default to be from a current-1 version to a current version.
5	Does your Solution support multiple versions of the product? If yes, please explain how many versions are supported.	Yes	CA Technologies supports the current GA and one previous version of our software.
6	Does your Solution include a description of the amount of time that a prior release is supported?	Yes	CA Technologies supports the current release, as well as the previous release. Customers are notified if CA plans to drop support on any given product; a one-year written notice is typically provided when this occurs.
7	Does your Solution include the delivery of test scripts to certify proper proper installation?	Yes	The solution comes with a sample application that can be used to verify proper installation.

8	Does your Solution include the delivery of aggregated bundles of updates, patches and service packs to simplify maintenance?	Yes	Please see response to Question 1 above.
9	Does your Solution's product releases included special conversion processes?	Yes	If an upgrade to a new version of CA software requires any data conversions, scripts or other tools will be provided to assist in the upgrade process.

K. TRAINING AND IMPLEMENTATION

	Requirements	A	B
1	Does your Solution include a list of the implementation services that are available?	Yes	PLEASE SEE OUR IMPLEMENTATION PLAN INFORMATION IN APPENDIX A 8 SERVICES EFFORT FOR COMMONWEALTH OF VA DMV
2	Does your Solution include a description of how many times your application has been deployed?	Yes	The CA AuthMinder and CA RiskMinder solutions have been installed in 100's of locations globally.

3	Does your Solution include a description of a typical implementation's approach, including kick-off calls, technical reviews, design reviews and user acceptance testing? If yes, please describe.	Yes	CA's implementation follows an industry standard process. The typical implementation process breaks down into several phases. These phases are similar across different sized projects. The overall phases are: 1. Project Setup: Preparation work, identification and assignment of resources and process planning and setup. 2. Requirements Architecture Design: Analysis of requirements. Identification of use cases, resultant workflows and solution specification finalization. 3. Installation and Configuration: Infrastructure pre-requisites installed / setup. Installation of the products and initial solution and integration testing. 4. Quality Assurance: Execution of test plans primarily performed / coordinated by customer with remediation of identified issues by CA. 5. Document Deployment: Operations Guide produced. Documentation of configuration, tuning, optimizations and other customizations. Backup of installation. 6. Training and Knowledge Transfer: Formal Operational, Developer, Admin, etc. training. Walk through of Operations Guide. 7. Production Deployment and Rollout: Prepare production environment and install, setup of the products. Perform Solution tests and User Acceptance Testing. 8. Project Closure: Introduce CA Tech Support with handover of open issues or next step items. Project closure meeting. The overall effort required is mainly determined by the following: – Number and type of applications to integrate with – Number of business processes – Number of locations to install in (main site and DR or multiple globally distributed sites) – Amount of customization needed for processes – For a typical set of requirements (web portal, integration with log-on, set-up of self-registration pages, main site + DR), the technical implementation takes 6 to 8 weeks and the overall elapsed project time including all phases mentioned above is typically between 4 and 6 months.
4	Does your Solution include examples of a typical implementation timeline including key activities, number of resources on client and supplier end and projected length of time for implementation?	Yes	As part of the standard methodology used, a project management plan is used to communicate the activities, assignments, and timeline of the implementation. This project plan is communicated to all during the kick-off and then kept current throughout the life of the project.

5	Does your Solution include a description of your organization's training approach?	Yes	CA Education offers flexible delivery methods including on-site training, virtual instructor-led training, and web-based training to maximize your investment in CA software. Our commitment to effective training is demonstrated in how we develop and deliver our curriculum. We will work with you to identify your educational needs and provide a range of flexible learning options to meet your goals. We've provided implementation and administration training as part of the training plan
6	Does your Solution include any methodology training?	No	We do not offer methodology training at this time.
7	Does your Solution include computer based-training modules?	No	Currently, we do not offer AuthMinder and RiskMinder CBT training modules.

EXHIBIT B PRICING
CONTRACT NUMBER VA-130131-CA
BETWEEN
VIRGINIA INFORMATION TECHNOLOGIES AGENCY
AND
CA, INC.

Exhibit B is hereby incorporated into and made an integral part of Contract Number VA-130131-CA ("Contract") between the Virginia Information Technologies Agency ("VITA" or "Commonwealth" or "State") and CA, INC. ("Supplier").

In the event of any discrepancy between this Exhibit B and Contract No. VA-130131-CA, the provisions of Contract No. VA-130131-CA shall control.

CA Pricing - Advanced Authentication *

Product	Metric	Product Code	Discounted Price	Annual Maintenance	Product Specific Notes
CA RiskMinder (Minimum 4,000 users)	Per User	ARCRFV990	$ 19.40	$ 3.88	Minimum quantity of 4,000 users required per procurement
CA AuthMinder (Minimum 4,000 users)	Per User	AUTHMV990	$ 25.49	$ 5.10	Minimum quantity of 4,000 users required per procurement
CA RiskMinder - Unlimited Term License	Term	ARCRFV990	TBD	TBD	Pricing for an Unlimited Term license of RiskMinder will be negotiated on a case-by-case basis
CA AuthMinder - Unlimited Term License	Term	AUTHMV990	TBD	TBD	Pricing for an Unlimited Term license of AuthMinder will be negotiated on a case-by-case basis
CA Arcot SMS Delivery of OTP	Transactional	ARCSDO99000	$ 0.08	N/A	Based on a transactional cost; annual maintenance doesn't apply
CA Arcot Voice Delivery of OTP	Transactional	ARCSVO99000	$ 0.15	N/A	Based on a transactional cost; annual maintenance doesn't apply

* - the above pricing assumes no previous purchase of AuthMinder or RiskMinder by the Commonwealth of VA.

CA Pricing - Advanced Authentication -- Based on Volume Discount **

Product	Metric	Product Code	Discounted Price	Annual Maintenance	Product Specific Notes
CA RiskMinder (Minimum 250,000 users)	Per User	ARCRFV990	$ 0.47	$ 0.09	Minimum purchase of 250,000 users
CA AuthMinder (Minimum 250,000 users)	Per User	AUTHMV990	$ 0.47	$ 0.09	
CA Arcot SMS Delivery of OTP	Transactional	ARCSDO99000	$ 0.08	N/A	Based on a transactional cost; annual maintenance doesn't apply
CA Arcot Voice Delivery of OTP	Transactional	ARCSVO99000	$ 0.15	N/A	Based on a transactional cost; annual maintenance doesn't apply

** - the above pricing assumes the Commonwealth of VA's initial purchase of at least 1.5M licenses to support CAS - this pricing is for additional capacity above & beyond the initial purchase of RiskMinder and AuthMinder.

CA Pricing - Services Components

Services Component	Metric	Product Code	Component Price	Annual Maintenance	Product Specific Notes
CA Scrambled Pin Pad - GD Component	Component	N/A	$ 15,000	$ 3,000	This product is delivered as a Global Delivery component
IBM TAM Connector (Risk/AuthMinder)	Component	N/A	$ 30,000	$ 6,000	This product is delivered as a Global Delivery component
IBM TAM Connector (Risk/AuthMinder)	Component	N/A	TBD via separate SOW	20% of Component Price	This product is delivered as a Global Delivery component

Advanced Authentication Training

Training Class	# of Days	Education Code	Price per Day	Total Price	Specific Notes
CA RiskMinder r2.2: Implementation 200	2	04RKF20011	$ 6,500	$ 13,000	Training for CA Advanced Authentication for up to 10 attendees
CA RiskMinder r2.2: Administration 200	3	04RKF20021	$ 6,500	$ 19,500	
CA AuthMinder r6.2: Implementation 200	1	04WBF20011	$ 6,500	$ 6,500	
CA AuthMinder r6.2: Administration 200	2	04WBF20021	$ 6,500	$ 13,000	

CA Pricing - ImplementationServices

Services	Metric	Code	Price		Specific Notes
RiskMinder Implementation Services	Project	N/A	TBD		Determined during scoping sessions
AuthMinder Implementation Services	Project	N/A	TBD		Determined during scoping sessions

2291 Wood Oak Drive
Herndon, VA 20171-2823
T +1 703 708 3000
F +1 703 709 4926

January 24, 2013

Mr. Michael Novak
Sourcing Specialist, Supply Chain Management
Virginia Information Technologies Agency (the “Commonwealth of Virginia”)
11751 Meadowville Lane
Chester, Virginia 23836

Re: <u>CA Source Code Escrow</u>

Dear Mr. Novak:

“**Escrow of Source Code.** CA has deposited a copy of the source code of the CA software with Iron Mountain Intellectual Property Management, Inc., 2100 Norcross Parkway, Suite 150, Norcross, Georgia, 30071, USA under the terms of the Custom Technology Deposit Account Services Agreement dated November 19, 2012 (the “Escrow Agreement”). In the event that the State becomes a licensee of the CA software, CA shall appoint the Commonwealth of Virginia as a beneficiary under the Escrow Agreement.

Very Truly Yours,

Tina Ratcliff
Director, Public Sector Contracts
CA, Inc

EXHIBIT D SOW TEMPLATE
CONTRACT NUMBER VA-130131-CA
BETWEEN
VIRGINIA INFORMATION TECHNOLOGIES AGENCY
AND
CA, INC.

Exhibit D is hereby incorporated into and made an integral part of Contract Number VA-130131-CA ("Contract") between the Virginia Information Technologies Agency ("VITA" or "Commonwealth" or "State") and CA, INC. ("Supplier").

In the event of any discrepancy between this Exhibit D and Contract No. VA-130131-CA, the provisions of Contract No. VA-130131-CA shall control

EXHIBIT D-X STATEMENT OF WORK (SOW) TEMPLATE
BETWEEN (NAME OF AUTHORIZED USER) AND CA, INC.

ISSUED UNDER

CONTRACT NUMBER VA-130131-CA
BETWEEN
VIRGINIA INFORMATION TECHNOLOGIES AGENCY
AND
CA,INC.

Exhibit D-X, between (Name of Agency/Institution) and CA, Inc. ("Supplier") is hereby incorporated into and made an integral part of Contract Number VA-130131-CA ("Contract") between the Virginia Information Technologies Agency ("VITA") on behalf of the Commonwealth of Virginia and Supplier.

In the event of any discrepancy between this Exhibit D-X and the Contract, the provisions of the Contract shall control.

[Note to Template Users: Instructions for using this template to draft a Statement of Work are in gray highlight and ***italics****. These instructions should be deleted after the appropriate text has been added to the Statement of Work. Contractual language is* ***not italicized*** *and should remain in the document. Text that is highlighted in blue is variable based on the nature of the project.]*

STATEMENT OF WORK

This Statement of Work (SOW) is issued by the (Name of Agency/Institution), hereinafter referred to as "Authorized User" under the provisions of the Contract,". The objective of the project described in this SOW is for the Supplier to provide the Authorized User with a Solution ("Solution") or Services ("Services)" or Software ("Software") or Hardware and Maintenance or Licensed Application Services" for Authorized User Project Name. *(Customize the last sentence to state what you are getting from the Supplier, based on the VITA Contract language, and with your project name.)*

1. PERIOD OF PERFORMANCE

The work authorized in this SOW will occur within XX (XX) months of execution of this Statement of Work. This includes delivery, installation, implementation, integration, testing and acceptance all of products and services necessary to implement the Authorized User's Solution, training, and any support, other than on-going maintenance services. The period of performance for maintenance services shall be one (1) year after implementation or end of Warranty Period and may be extended for additional one (1) year periods, pursuant to and unless otherwise specified in the Contract. *(Customize this section to match what you are getting from the Supplier, based on the allowable scope of the VITA Contract and your project's specific needs within that allowable scope.)*

2. PLACE OF PERFORMANCE

(Assign performance locations to major milestones or any other project granularity, depending on your transparency and governance needs, if needed.)

Tasks associated with this project will be performed at the Authorized User's location(s) in City/State, at Supplier's location(s) in City/State, or other locations as required by the effort.

3. PROJECT DEFINITIONS

Provide project unique definitions so that all stakeholders have the same understanding. Ensure these do not conflict with the Contract definition.).

All definitions of the Contract shall apply to and take precedence over this SOW. Authorized User's specific project definitions are listed below:

4. PROJECT SCOPE

(Provide a description of the scope of your project and carve out what is NOT in the scope of your project. Remember that it must fit within the VITA Contract scope.).

A. General Description of the Project Scope

B. Project Boundaries

5. AUTHORIZED USER'S SPECIFIC REQUIREMENTS

(Provide information about your project's and your agency's specific requirements for this particular project including, but not limited to the following subsections):

A. Authorized User-Specific Requirements

B. Special Considerations for Implementing Technology at Authorized User's Location(s)

C. Other Project Characteristics to Insure Success

6. CURRENT SITUATION

(Provide enough background information to clearly state the current situation to Supplier so that Supplier cannot come back during performance claiming any unknowns or surprises. Some example subsections are provided below. You may collapse/expand as you feel is necessary to provide adequate information and detail.)

A. Background of Authorized User's Business Situation

B. Current Architecture and Operating System

C. Current Work Flow/Business Flow and Processes

D. Current Legacy Systems

E. Current System Dependencies

F. Current Infrastructure (Limitations, Restrictions)

G. Usage/Audience Information

7. PRODUCTS AND SERVICES TO SUPPORT THE PROJECT REQUIREMENTS (AND/OR SOLUTION)

A. Required Products (or Solution Components)

(List the products, or if your project is for a Solution, the Solution components, (hardware, software, etc.) provided by Supplier that will be used to support your project requirements. Identify any special configuration requirements, and describe the system infrastructure to be provided by the Authorized User. Provide an overview that reflects how the system will be deployed within the Authorized User's environment. You are urged to refer to the VITA Contract for allowable scope and other guidance in drafting language for this section.)

B. Required Services

(*List the services (e.g., requirements development, Solution design, configuration, interface design, data conversion, installation, implementation, testing, training, risk assessment, performance assessment, support and maintenance) that will be provided by Supplier in the performance of your project. You are urged to refer to the VITA Contract for the definition of Services and for the allowable scope in drafting language for this section. You will notice subsections "C" and "D" below offer areas for expanded detail on training, support and maintenance services. You may add other subsections in which you wish to expand the information/details/requirements for other service areas as well. It is likely some of this detail will be a combination of your known needs and the Supplier's proposal. In all cases the provisions should include all negotiated commitments by both parties, even if you reference by incorporation the Supplier's proposal in any subsection.)*

C. Training Requirements and/or Authorized User Self-Sufficiency/Knowledge Transfer

(*Provide an overview and details of training services to be provided for your project and any special requirements for specific knowledge transfer to support successful implementation of the Solution. If the intent is for the Authorized User to become self-sufficient in operating or maintaining the Solution, determine the type of training necessary, and develop a training plan, for such user self-sufficiency. Describe how the Supplier will complete knowledge transfer in the event this Statement of Work is not completed due to actions of Supplier or the non-appropriation of funds for completion affecting the Authorized User. You may refer to the VITA Contract for guidance on the allowable scope for this.*

D. Support and Maintenance Requirements

(*Document the level of support, as available under the Contract, required by your project to operate and maintain the Solution. This may include conversion support, legacy system integration, transition assistance, Solution maintenance (including maintenance level), or other specialized consulting to facilitate delivery or use of the Solution.*

E. Personnel Requirements

(*Provide any supplier personnel qualifications, requirements, licenses, certifications or restrictions including project manager, key personnel, subcontractors, etc., but ensure they do not conflict with the VITA Contract terms.)*

F. Transition Phase-In/Phase-Out Requirements

(*Describe any specific requirements for orientation or phasing in and/or phasing out of the project with the Supplier. Be specific on what the project needs and expected results are, the duration and other pertinent detail, but ensure they do not conflict with the VITA Contract provision(s) regarding Transition of Services or with any other training requirements in the SOW.)*

8. TOTAL PROJECT PRICE

The total Fixed Price for this Project shall not exceed $US XXX.

Supplier's invoices shall show retainage of ____________ Following completion of Solution implementation, Supplier shall submit a final invoice to the Authorized User, for the final milestone payment amount shown in the table in section 9 below, plus the total amount retained by the Authorized User. If travel expenses are not included in the fixed price of the Solution, such expenses shall be reimbursed in accordance with Commonwealth of Virginia travel policies as published by the Virginia Department of Accounts (http://www.doa.virginia.gov). In order to be reimbursed for travel expenses, Supplier must submit an estimate of such expenses to Authorized User for approval prior to incurring such expenses.

(*Sections 9 through 11 should be used or deleted depending on the project's complexity, risk and need for governance. For a simple project you may only need the section 10 table, but for a more complex project, or a major IT project, you may need a combination of or all of the tables for check and balance and redundancy.*)

9. PROJECT DELIVERABLES

(*Provide a list of Supplier's deliverable expectations. The table is to be customized for the Authorized User's project. You may want to categorize deliverables for each phase or major milestone of the project and then categorize other interim deliverables and/or performance and status reports under one of them or under an Administrative or Project Management section.)*

The following deliverables are to be provided by Supplier under this SOW. Subsequent sections may include further detail on the content requirements for some deliverables.

No.	Title	Due Date	Format Required (i.e., electronic/hard copy/CD/DVD	Distribution Recipients	Review Complete Due Date	Final Due Date
	Project Plan					
	Design Plan					
	Implementation Plan					
	Data Conversion Plan					
	Risk Assessment Plan					
	Test Plan					
	Training Plan					
	Performance Plan					
	Contingency Plan					
	Disaster Recovery Plan					
	Cutover Plan					
	Change Management Plan					
	Transition Plan					
	Monthly Status Reports					

	Quarterly Performance /SLA Reports					
	Training Manual					
	Final Solution Submission Letter					
	Final Acceptance Letter					

10. MILESTONES, DELIVERABLES, PAYMENT SCHEDULE, AND HOLDBACKS

(*This table should include the project's milestone events, associated deliverables, when due, milestone payments, any retainage amount to be held until final acceptance and the net payment you promise to pay for each completed and accepted milestone event. This table includes sample data only and must be customized for your project needs.)*

The following table identifies milestone events and deliverables, the associated schedule, any associated payments, any retainage amounts, and net payments.

Milestone Event	Associated Milestone Deliverable(s)	Schedule	Payment	Retainage	Net Payment
Project kick-off meeting	---		---	---	---
			---	---	---

	---		---	---	---

				--	
Final Acceptance			--	--	

11. EVENTS AND TASKS FOR EACH MILESTONE

(*If needed, provide a table of detailed project events and tasks to be accomplished to deliver the required milestones and deliverables for the complete Solution. Reference each with the relevant milestone. A Work Breakdown Structure can be used as shown in the table below or at the very least a Project Plan should have this granularity. The Supplier's proposal should be tailored to the level of detail desired by the Authorized User's business owner/project manager for project governance.)*

The following table identifies project milestone events and deliverables in a Work Breakdown Structure format.

WBS No.	Milestone	Milestone Event	Milestone Task	Interim Task Deliverables	Duration
1.0					
1.1					

1,1,1					
1.1.2					
1.2					

12. ACCEPTANCE CRITERIA

(*This section should reflect the mutually agreed upon UAT and Acceptance Criteria specific to this engagement. Please read the VITA contract definitions for the definitions or Requirements and Acceptance. Ensure the language in this section does not conflict with the VITA Contract language.)*

Acceptance Criteria for this Solution will be based on a User Acceptance Test (UAT) designed by Supplier and accepted by the Authorized User. The UAT will ensure that all of the requirements and functionality required for the Solution have been successfully delivered. Supplier will provide the Authorized User with a detailed test plan and acceptance check list based on the mutually agreed upon UAT Plan. This UAT Plan check-list is incorporated into this SOW in Exhibit B-X.

Each deliverable created under this Statement of Work will be delivered to the Authorized User with a Deliverable Acceptance Receipt. This receipt will describe the deliverable and provide the Authorized User's Project Manager with space to indicate if the deliverable is accepted, rejected, or conditionally accepted. Conditionally Accepted deliverables will contain a list of deficiencies that need to be corrected in order for the deliverable to be accepted by the Project Manager. The Project Manager will have ten (10) days from receipt of the deliverable to provide Supplier with the signed Acceptance Receipt unless an alternative schedule is mutually agreed to between Supplier and the Authorized User in advance.

13. PROJECT ASSUMPTIONS AND PROJECT ROLES AND RESPONSIBILITIES

(This section contains areas to address project assumptions by both the Supplier and the Authorized User and to assign project-specific roles and responsibilities between the parties. Make sure that all assumptions are included to alleviate surprises during the project. Ensure that all primary and secondary (as needed) roles and responsibilities are included. You will tailor the Responsibility Matrix table below to fit your project's needs.)

A. Project Assumptions

The following assumptions are specific to this project:

B. Project Roles and Responsibilities

The following roles and responsibilities have been defined for this project:

(Sample Responsibility Matrix)

Responsibility Matrix	Supplier	Authorized User
Infrastructure – Preparing the system infrastructure that meets the recommended configuration defined in Section 2B herein		√
Server Hardware		√
Server Operating		√
Server Network Connectivity		√
Relational Database Management Software (Installation and Implementation)		√
Server Modules – Installation and Implementation	√	
PC Workstations – Hardware, Operating System, Network Connectivity		√
PC Workstations – Client Software		√
Application Installation on PC Workstations	√	
Wireless Network Access Points	√	

Cabling, Electric and User Network Connectivity from Access Points		√
Wireless Mobile Computing Products – Scanners, printers	√	
Project Planning and Management	√	√
Requirements Analysis	√	√
Application Design and Implementation	√	
Product Installation, Implementation and Testing	√	
Conversion Support	√	
Conversion Support -- Subject Matter Expertise		√
Documentation	√	
Training	√	
Product Maintenance and Support	√	
Problem Tracking	√	√
Troubleshooting – IT Infrastructure		√
Troubleshooting – Solution	√	

14. COMMONWEALTH AND SUPPLIER-FURNISHED MATERIALS, EQUIPMENT, FACILITIES AND PROPERTY

(*In this section, provide details of any materials, equipment, facilities and property to be provided by your Agency or the Supplier in performance of this project. If none, so state so that the requirements are clear. If delivery of any of these is critical to the schedule, you may want to identify such delivery with hard due dates tied to "business days after project start' or "days after event/milestone." Be sure to specify the delivery and point of contact information.)*

A. PROVIDED BY THE COMMONWEALTH

B. PROVIDED BY THE SUPPLIER

15. SECURITY REQUIREMENTS

(Provide (or reference as an Attachment) Authorized User's security requirements.)

For any individual Authorized User location, security procedures may include but not be limited to: background checks, records verification, photographing, and fingerprinting of Supplier's employees or agents. Supplier may, at any time, be required to execute and complete, for each individual Supplier employee or agent, additional forms which may include non-disclosure agreements to be signed by Supplier's employees or agents acknowledging that all Authorized User information with which such employees and agents come into contact while at the Authorized User site is confidential and proprietary. Any unauthorized release of proprietary information by the Supplier or an employee or agent of Supplier shall constitute a breach of the Contract.

Supplier shall comply with all requirements in the Security Compliance section of the Contract

16. REQUIRED STANDARDS, CERTIFICATIONS AND SPECIFICATIONS

In addition to any standards and specifications included in the Contract, Supplier shall follow the standards and specifications listed below during performance of this effort.

(List any specific Commonwealth, VITA, Federal, engineering, trade/industry or professional standards, certifications and specifications that Supplier is required to follow or possess in performing this work. The first bullet includes a link to COVA-required standards for all Commonwealth technology projects. The rest are examples only and highlighted to reflect this. If you need an exception of any COVA-required standard, please follow the process located at this link: http://www.vita.virginia.gov/oversight/default.aspx?id=10344 and select the Data Standards Guidance bulleted link. Your AITR can assist you.

- COV ITRM Policies and Standards: http://www.vita.virginia.gov/library/default.aspx?id=537
- IEEE 802®
- HIPAA
- SAS 70 Type II

17. U.S. ENVIRONMENTAL PROTECTION AGENCY'S AND DEPARTMENT OF ENERGY'S ENERGY STAR GUIDELINESRISK MANAGEMENT

(Risk is a function of the probability of an event occurring and the impact of the negative effects if it does occur. Negative effects include schedule delay, increased costs, failure of dependent legacy system interoperability, other project dependencies that don't align with this project's schedule, and poor quality of deliverables. Depending on the level of risk of this project, as assessed by your Project Manager and/or Steering Committee, this section may contain any or all of the following components, at a level of detail commensurate with the level of risk. Remember to add them to the Deliverables table.)

C. Initial Risk Assessment

Authorized User and Supplier shall each provide an initial assessment from their point of view.

D. Risk Management Strategy

(The list below is taken from VITA PMD template discussing what should go into a Risk Management Strategy. Don't forget to consider and plan for any budget contingencies to accommodate potential risks that are identified.)

1. **Risk Identification Process:** The processes for risk identification.
2. **Risk Evaluation and Prioritization**: How risks are evaluated and prioritized.
3. **Risk Mitigation Options**: Describe the risk mitigation options. They must be realistic and available to the project team.
4. **Risk Plan Maintenance:** Describe how the risk plan is maintained during the project lifecycle.
5. **Risk Management Responsibilities:** Identify all project team members with specific risk management responsibilities. (e.g., an individual responsible for updating the plan or an individual assigned as a manager).

E. Risk Management Plan

(*Include a description of frequency and form of reviews, project team responsibilities, steering and oversight committee responsibilities and documentation. Be sure to add all deliverables associated with risk strategizing and planning to the list of Deliverables.)*

18. DISASTER RECOVERY

Planning for disaster recovery for your project is paramount to ensure continuity of service. The criticalness and complexity of your project, including its workflow into other dependent systems of the Commonwealth or federal systems, will help you determine if you require a simple contingency plan or a full-blow contingency plan that follows the Commonwealth's ITRM Guideline SEC508-00 found at this link:

http://www.vita.virginia.gov/uploadedFiles/Library/ContingencyPlanningGuideline04_18_2007.pdf

It is advisable that you visit the link before making your decision on how you need to address contingency planning and related deliverables in this SOW; as well as, how this will impact your planned budget. A likely deliverable for this section would be a Continuity of Operations Plan. You may choose to include the above link in your final SOW to describe what the Plan will entail. The same link includes the following processes, which you may choose to list in your final requirements for this section, to be performed by your team, the Supplier or both and/or a steering committee if your project warrants such oversight and approval:

- *Development of the IT components of the Continuity of Operations Plan (COOP)*
- *Development and exercise of the IT Disaster Recovery Plan (IT DRP) within the COOP*
- *Development and exercise of the IT System Backup and Restoration Plan*

19. PERFORMANCE BOND

(*If your project is sizeable, complex and/or critical, and the VITA Contract does not already provide for a performance bond, you may want the Supplier to provide one. The VITA Contract may include an Errors and Omissions insurance requirement, which would cover the Supplier's liability for any breach of the Contract or this SOW. Be sure to read the Contract for this information. However, if you feel that this project warrants further performance incentive due to the project or the Supplier's viability, you may include the following language in this section.)*

____

20. OTHER TECHNICAL/FUNCTIONAL REQUIREMENTS

(Provide any other unique project technical and functional requirements and expectations in sufficient detail in this section. Ensure they do not conflict with existing requirements in the VITA Contract. Several examples are listed.)

F. ________________________________

G. ________________________________

H. ________________________________

I. ________________________________

21. REPORTING

(*The following are examples of reporting requirements which may be included in your SOW depending on the project's need for governance. In an effort to help VITA monitor Supplier performance, it is strongly recommended that the SOW include "Supplier Performance Assessments". These assessments may be performed at the Project Manager's discretion and are not mandated by VITA.)*

A. Weekly/Bi-weekly Status Update.

The weekly/bi-weekly status report, to be submitted by Supplier to the Authorized User, should include: accomplishments to date as compared to the project plan; any changes in tasks, resources or schedule with new target dates, if necessary; all open issues or questions regarding the project; action plan for addressing open issues or questions and potential impacts on the project; risk management reporting.

B. Supplier Performance Self-Assessment.

Within thirty (30) days of execution of the project start, the Supplier and the Authorized User will agree on Supplier performance self-assessment criteria. Supplier shall prepare a monthly self-assessment to report on such criteria. Supplier shall submit its self-assessment to the Authorized User who will have five (5) days to respond to Supplier with any comments. If the Authorized User agrees with Supplier's self-assessment, such Authorized User will sign the self-assessment and submit a copy to the VITA Supplier Relationship Manager.

C. Performance Auditing

(If you have included service level requirements in the above section entitled, Other Technical/Functional Requirements, you will want to include a requirement here for your ability to audit the results of the Supplier's fulfillment of all requirements, Likewise, you may want to include your validation audit of the Supplier's performance reporting under this Reporting section. It is important, however, that you read the VITA contract prior to developing this section's content so that

conflicts are avoided. Suggested language is provided below, but must be customized for your project.)

____. *(If none, you may add your escalation procedure in this section.)*

D. Supplier Performance Assessments

(You may want to develop assessments of the Supplier's performance and disseminate such assessments to other Authorized Users of the VITA Contract. Prior to dissemination of such assessments, Supplier will have an opportunity to respond to the assessments, and independent verification of the assessment may be utilized in the case of disagreement.)

22. CHANGE MANAGEMENT

(*Changes to the baseline SOW must be documented for proper project oversight. Depending on your project, you may need to manage and capture changes to configuration, incidents, deliverables, schedule, price or other factors your team designates as critical. Any price changes must be done in compliance with the Code of Virginia, § 2.2-4309. Modification of the contract, found at this link: http://leg1.state.va.us/cgi-bin/legp504.exe?000+coh+2.2-4309+500825. Changes to the scope of this SOW must stay within the boundaries of the scope of the VITA Contract.*

For complex and/or major projects, it is recommended that you use the VITA PMD processes and templates located at: http://www.vita.virginia.gov/oversight/projects/default.aspx?id=567. Administrative or non-technical/functional changes (deliverables, schedule, point of contact, reporting, etc.) should extrapolate the affected sections of this SOW in a "from/to" format and be placed in a numbered modification letter referencing this SOW and date, with a new effective date. The VITA Contract may include a template for your use or you may obtain one from the VITA Contract's Point of Contact. It is very important that changes do not conflict with, but do comply with, the VITA Contract, which takes precedence. The following language may be included in this section, but additional language is needed to list any technical/functional change management areas specific to this SOW; i.e., configuration, incident, work flow, or any others of a technical/functional nature.)

All changes to this SOW must comply with the Contract. Price changes must comply with the Code of Virginia, § 2.2-4309. Modification of the contract, found at this link: http://leg1.state.va.us/cgi-bin/legp504.exe?000+coh+2.2-4309+500825

All changes to this SOW shall be in written form and fully executed between the Authorized User's and the Supplier's authorized representatives. For administrative changes, the parties agree to use the change template, attached to this SOW. For technical/functional change management requirements, listed below, the parties agree to follow the processes and use the templates provided at this link: http://www.vita.virginia.gov/oversight/projects/default.aspx?id=567

23. POINT OF CONTACT

For the duration of this project, the following project managers shall serve as the points of contact for day-to-day communication:

Authorized User: ______________________________

Supplier: ______________________________

By signing below, both parties agree to the terms of this Exhibit.

Supplier:	**Authorized User:**
____	____
(Name of Supplier)	(Name of Agency/Institution)

By: ________________________________

(Signature)

Name: _____________________________

(Print)

Title: ______________________________

Date: ______________________________

By: __________________________________

(Signature)

Name: _______________________________

(Print)

Title: _________________________________

Date: __________________________________

EXHIBIT E CHANGE ORDER TEMPLATE
CONTRACT NUMBER VA-130131-CA
BETWEEN
VIRGINIA INFORMATION TECHNOLOGIES AGENCY
AND
CA, INC.

Exhibit E is hereby incorporated into and made an integral part of Contract Number VA-130131-CA ("Contract") between the Virginia Information Technologies Agency ("VITA" or "Commonwealth" or "State") and CA, INC. ("Supplier").

In the event of any discrepancy between this Exhibit E and Contract No. VA-130131-CA, the provisions of Contract No. VA-130131-CA shall control.

This Change Order No. XXX hereby modifies and is made an integral part of Statement of Work E-X ("SOW"), between NAME OF AGENCY/INSTITUTION ("Authorized User") and CA, Inc.,("Supplier"), which was issued under Contract Number VA-130131-CA ("Contract") between the Virginia Information Technologies Agency ("VITA") and Supplier, on behalf of the Commonwealth of Virginia and its Authorized Users.

[*Note: Instructions for using this template to draft a Change Order are in gray. These instructions should be deleted after the appropriate text has been added to the Change Order. Contractual language is not in gray and should remain in the document. Text that is highlighted in blue is contractual language that is variable based on the nature of the project and in final form should not be highlighted. Agency/Institution should remove the first two lines of the heading, which pertain to this template as an Exhibit to the VITA Contract and remove the Exhibit reference from the header.*]

CHANGE ORDER

This is Change Order No. XXX to a SOW issued by Authorized User to Supplier under which Supplier is to provide the Authorized User with a Authorized User Project Name Solution ("Solution").

The following item(s) is/are hereby modified as follows: *[Note: Include only the sections of the SOW that are being changed. Do not include sections not being modified. Changes should be clearly identified as "From" (copy/paste from current SOW section) and "To" (fully describe the change(s) to the referenced section). Here is an example, using SOW section 1.]*

1. PERIOD OF PERFORMANCE

This Change Order No. XXX is issued pursuant to and, upon execution, shall become incorporated in the SOW, which is incorporated in the Contract. In the event of conflict, the following order of precedence shall apply:

i). The Contract

ii). Statement of Work E-X, as amended by this and previous Change Orders, with the more current Change Orders superseding older Change Orders.

The foregoing is the complete and final expression of the agreement between the parties to modify the SOW and cannot be modified, except by a writing signed by duly authorized representatives of both parties hereto.

ALL OTHER TERMS AND CONDITIONS OF THE REFERENCED SOW REMAIN UNCHANGED.

By signing below, the authorized parties agree to the terms of this Change Order No.XXX, effective (INSERT EFFECTIVE DATE).

Supplier

By: ________________________________

(Signature)

Name: ______________________________

(Print)

Title: ______________________________

Date: ______________________________

Authorized User

By: __________________________________

(Signature)

Name: _______________________________

(Print)

Title: _________________________________

Date: _________________________________

EXHIBIT F RESERVED
CONTRACT NUMBER VA-130131-CA
BETWEEN
VIRGINIA INFORMATION TECHNOLOGIES AGENCY
AND
CA, INC.

EXHIBIT G LOBBYING CERTIFICATION
CONTRACT NUMBER VA-130131-CA
BETWEEN
VIRGINIA INFORMATION TECHNOLOGIES AGENCY
AND
CA, INC.

Exhibit G is hereby incorporated into and made an integral part of Contract Number VA-130131-CA ("Contract") between the Virginia Information Technologies Agency ("VITA" or "Commonwealth" or "State") and CA, INC. ("Supplier").

In the event of any discrepancy between this Exhibit G and Contract No. VA-130131-CA, the provisions of Contract No. VA-130131-CA shall control.

CERTIFICATION REGARDING LOBBYING

The undersigned certifies, to the best of his or her knowledge and belief, that:

No Federal appropriated funds have been paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee or an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal Contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal Contract, grant, loan, or cooperative agreement.

If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal Contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit standard Form-LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions.

The undersigned shall require that the language of this certification be included in the award documents for all sub awards at all tiers (including subcontracts, sub grants, and Contracts under grants, loans and cooperative agreements) and that all sub recipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by Section 1352, title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure.

Signature: Iwalm Ratcliff

Printed Name: **Tina Ratcliff**

Organization: **CA, Inc.**

Date: 1/24/13

EXHIBIT H CA ORDER FORM
CONTRACT NUMBER VA-130131-CA
BETWEEN
VIRGINIA INFORMATION TECHNOLOGIES AGENCY
AND
CA, INC.

Exhibit H is hereby incorporated into and made an integral part of Contract Number VA-130131-CA ("Contract") between the Virginia Information Technologies Agency ("VITA" or "Commonwealth" or "State") and CA, INC. ("Supplier").

In the event of any discrepancy between this Exhibit H and Contract No. VA-130131-CA, the provisions of Contract No. VA-130131-CA shall control.

CA, Inc., 2291 Wood Oak Drive Herndon, Virginia 20171 ("CA")

Effective Date of this Order Form:		
Customer Name: (which may be referred to as "Customer" or "You" or "Licensee" in the referenced Agreement below)		Customer ID No:
Customer Address:		
Billing Address:		
Billing Contact:	Phone:	E-mail:
Shipment Address:		
Shipping Contact:	Territory: (if blank, US only)	
Technical Contact:	Phone:	E-mail:

If You are ordering CA Software, name of referenced agreement: ("Master Agreement" with respect to CA Software and CA Support and Maintenance)	Agreement No.:
If You are ordering CA Services, name of referenced agreements: ("Master Services Agreement" with respect to CA Services)	Agreement No.:
If You are ordering CA Education, name of referenced agreements: ("Master Education Agreement" with respect to CA Education)	Agreement No.:
Indicate here if there are changes to the terms of any of the referenced agreements in this Order Form: Master Agreement □; Master Services Agreement □; Master Education Agreement □. All such changes to this applicable Agreement stated in the referenced agreements shall apply to this Order Form unless stated otherwise.	For Customer Administrative Purposes Only: PO Required? No PO #:

THIS ORDER FORM COVERS:

CA SOFTWARE (WHICH MAY BE REFERRED TO AS "LICENSED PROGRAM", "SOFTWARE", OR "PRODUCT") LICENSED BY THE CUSTOMER FROM CA LIMITED BY THE SPECIFIC AUTHORIZED USE LIMITATION BASED ON THE LICENSING MODEL STATED AND/OR THE SUPPORT PROVIDED ARE GOVERNED BY (I) THIS ORDER FORM, (II) THE MASTER AGREEMENT SPECIFIED ABOVE, (III) CA SUPPORT POLICY AND TERMS, LOCATED AT HTTP://SUPPORT.CA.COM WHERE SUPPORT IS PROVIDED, AND (IV) THE SPECIFIC PROGRAM DOCUMENTATION ("SPD") FOR SPECIFIED CA SOFTWARE AND/OR SUPPORT LOCATED AT HTTP://WWW.CA.COM/LICENSEAGREEMENT (TOGETHER REFERRED TO AS "AGREEMENT" WITH RESPECT TO CA SOFTWARE AND/OR SUPPORT).

CA Order Form

ANY CA SERVICES OR EDUCATION ORDERED IS GOVERNED BY (I) THIS ORDER FORM, (II) THE MASTER SERVICES AGREEMENT OR MASTER EDUCATION AGREEMENT SPECIFIED ABOVE, (III) THE CA SERVICES POLICY AND TERMS LOCATED AT HTTP://WWW.CA.COM/SERVICES/POLICIES OR CA EDUCATION POLICY AND TERMS LOCATED AT HTTP://CA.COM/EDUCATION/TERMS (WHICHEVER IS APPLICABLE) AND (IV) THE APPLICABLE CA SERVICES OR EDUCATION SPECIFIC PROGRAM DOCUMENTATION ("SPD"), LOCATED AT HTTP://WWW.CA.COM/LICENSEAGREEMENT OR ATTACHED TO THIS ORDER FORM AS AN EXHIBIT (TOGETHER REFERRED TO AS "AGREEMENT" WITH RESPECT TO CA SERVICES AND/OR CA EDUCATION.

The pricing and terms offered herein expire unless Customer executes and delivers this order to CA prior to 5pm Eastern Time on , however this provision shall be null and void and have no legal effect if this order is countersigned by CA. In the event a payment due date falls on a weekend or a holiday the payment shall be payable by the Customer to CA on the business day immediately prior to such date.

Payment Profile

Due Date	Lic./Subscription Fee	Support Fee	Services Fee/Education Fee	Total Fees Due

***See complete Services and Education fee information below.**

CA Distributed Software Information (USD)

Product Name	Support	License Type*	Operating System	Authorized Use Limitation	Start Date**	End Date	Ship (Y/N)	License Fee or Subscription Fee	Support Fee	Optional First Year Stated Renewal

Distributed Software Fee	**Total Fee (USD)**
License Fee	$000
Support Fee	$000
Optional First Year Stated Renewal Fee	$000

*With respect to perpetual licenses, Start Date and End Date refer to the start date and end date for Support.

**If no date stated, the start date is the Effective Date of the Order Form. The dates set out in the CA Software tables shall in no way be deemed to impact or change the Effective Date of this Order Form. All amounts are exclusive of taxes which will be payable in addition to the fees listed above.

Any CA Software identified with "NO" under the heading entitled "Ship" above was previously delivered to Customer by CA and therefore will not be delivered to Customer again. CA Software identified with a "YES" will be delivered to Customer following execution of this order. The CA Software shall be delivered either by electronic delivery ("ESD") or if CA requires in tangible media CPT, as defined in INCOTERMS 2010, from CA's shipping point. CA agrees to be responsible for all customs duties and clearances and title to any CA hardware if included will pass upon point of delivery to carrier at CA's shipping location. In the event of electronic delivery, no tangible personal property will be delivered. Such electronic delivery may not automatically provide for an exemption from applicable sales or use tax. Any operating system identified as "Generic" or "GA" denotes such operating systems for which the CA Software is made generally available by CA in accordance with CA current published specifications.

Education Course Table

Product Code/ Material ID	**Course Code**	**Course Title**	**Delivery Format**	**# of Students**	**Class Date (if provided)**	**Duration (hours)**	**Discount (%)**	**Fees**

CA Services and Education Information (USD):

CA Services or Education Description	Quantity	Variables (Users, Roles, App servers; students)	Fixed Price or Time and Materials	**Fees**

[Name of CA Services or Education Course]				
[Name of CA Services or Education Course]				
[Name of CA Services or Education Course]				

CA Services and Education Payment Profile:	**Course Description / Milestone Description**	**Fees Due** USD
Order Form 1/31/2013		$
Invoice Milestone 1		$
Invoice Milestone 2		$
Invoice Milestone 3		$
Invoice Milestone 4		$
Invoice Milestone 5		$
Invoice Milestone 6		$
	Total CA Fees Due	$

For Fixed Price, upon completion of a Milestone, Customer will be invoiced the applicable fee for such Milestone as stated above. The Fixed Fee(s) above is only available for the scope of Services set forth herein.

CA shall have the right to increase the Time and Material rates or Fixed Price for any Change Request that modifies the scope of Services, or if the Project has not commenced within three (3) months of the Effective Date specified herein, or if project activity is not in accordance with the agreed upon work plan.

Invoices are due and payable as per the terms of the referenced Master Agreement or thirty (30) days from the date of invoice. In addition to the Services fees and, if applicable, the Education fees listed above, Customer agrees to pay any applicable tariffs, levies, duties or taxes.

All Education Course Fees and /or Training Credits Purchased are due and payable in full upon execution of this Order Form. You acknowledge and agree that you are required to draw down the Educational Funds set forth in the Order Form if otherwise unspecified prior to the Term End Date of one (1) year from the Effective Date of the Order Form. No refunds will be available for any unused portion of the Educational Funds.

The following additional terms shall modify the Master Agreement: ***[NOTE: These clauses should be deleted if found in the underlying referenced agreements. If this is a new customer using the online CA Master Agreement, only paragraphs "Press Release", "Reference Program", "Initial Payment" need to be added.]***

1.

[NOTE: Paragraphs "New Product Clause Exclusion" and "Limited Warranty" are only for NEW DISTRIBUTED product transactions. These clauses can be deleted for renewals and additional capacity transactions.]

2. THE FOLLOWING PARAGRAPH IS ONLY USED IF BUYING EDUCATION AS PART OF THE MAINFRAME ELA RENEWAL PROGRAM AND(i) THERE IS NO SERVICES OR EDUCATION MASTER AGREEMENT REFERENCED; AND, (ii) CA NEEDS TO REFERENCE A LICENSE AGREEMENT. PLEASE THEN COMPLETE THE REFERENCE INFORMATION TABLE FOR EDUCATION BY INSERTING THE LICENSE AGREEMENT NAME OR LICENSE AGREEMENT AS THE NAME OF THE REFERENCED AGREEMENT AND THE APPLICABLE LICENSE AGREEMENT NUMBER AS THE AGREEMENT NUMBER AND ADD THE FOLLOWING PROVISION]

   CA will use its reasonable best efforts to provide the education services hereunder in accordance with industry standards. **EXCEPT FOR THE WARRANTY IN THE PRECEDING SENTENCE, CA MAKES NO OTHER WARRANTY, EXPRESS OR IMPLIED AND DISCLAIMS ANY OTHER WARRANTIES OR CONDITIONS, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY AND FITNESS FOR A PARTICULAR PURPOSE. WITH RESPECT TO THIS EDUCATION, TO THE FULL EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL CA OR ITS SUPPLIERS BE LIABLE TO YOU OR ANYONE ELSE FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, EXEMPLARY, OR PUNITIVE DAMAGES, LOST PROFITS, LOST REVENUES, LOSS OF GOODWILL, LOST SAVINGS, OR LOST DATA, EVEN IF CA OR ITS SUPPLIERS HAVE BEEN ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH DAMAGES. IF THE ABOVE LIABILITY LIMITATION AND/OR EXCLUSION IS FOUND TO BE INVALID UNDER APPLICABLE LAW, THEN CA AND ITS SUPPLIER'S LIABILITY FOR SUCH CLAIM SHALL BE LIMITED TO THE AMOUNT OF THE FEES YOU HAVE ACTUALLY PAID FOR THE EDUCATION SERVICES GIVING RISE TO THE CLAIM. IN ALL OTHER RESPECT CA'S LIABILITY FOR DIRECT DAMAGES, HOWSOEVER ARISING, SHALL BE LIMITED TO THE FEES PAID FOR THE EDUCATION SERVICES GIVING RISE TO THE CLAIM. TO THE EXTENT SUCH ABOVE EXCLUSIONS OR LIMITATIONS ARE INVALID UNDER**

APPLICABLE LAW, THE ABOVE SUCH EXCLUSIONS AND LIMITATIONS SHALL NOT APPLY. ALL INTELLECTUAL PROPERTY RIGHTS REMAIN WITH CA OR ITS LICENSORS.

3. (Insert additional terms if applicable)
Product License Language
The Services provided are to implement the pre-existing features and functions of CA Arcot Software and do not include any customization or development activity that impacts any of the full features and benefits and underlying source code of the stand-alone CA Arcot Software. The payment of license fees for the CA Arcot Software is separate from the Services and will be made in accordance with the Acceptance plan set forth in the attached SOW.
4.

Each Agreement, including any attached exhibits, constitutes the entire agreement of the parties and supersedes all prior communications, understandings and agreements relating to its respective subject matter, whether oral or written. No modification or claimed waiver of any provision herein shall be valid except by written amendment signed by authorized representatives of Customer and CA. Any conflict or inconsistency among or between the terms and conditions of the documents comprising the respective agreement(s), with respect to CA Software, CA Education and/or CA Services, shall be resolved according to the following order of precedence, from the document with the greatest control to the least: (1) the Order Form; (2) the relevant SPD; (3) the relevant CA Policy and Terms Document; (4) the Master Agreement, The Master Services Agreement and the Master Education Agreement, as applicable; and (5) the Documentation for the relevant CA Software.

DIV OF MOTOR VEHICLES		**CA, Inc.**	
Signature:	______________________	Signature:	______________________
Name:	______________________	Name:	______________________
Title:	______________________	Title:	______________________
Date	______________________	Date:	______________________

Services Exhibit

Replace this Statement with Needed Content.

EXHIBIT I – CA DOCUMENTATION

CONTRACT NUMBER VA-130131-CA

BETWEEN

VIRGINIA INFORMATION TECHNOLOGIES AGENCY

AND

CA, INC.

Exhibit I is hereby incorporated into and made an integral part of Contract Number VA-130131-CA (“Contract”) between the Virginia Information Technologies Agency (“VITA” or “Commonwealth” or “State”) and CA, INC. (“Supplier”).

In the event of any discrepancy between this Exhibit E and Contract No. VA-130131-CA, the provisions of Contract No. VA-130131-CA shall control.

1. CA Arcot-RiskFort – 3.0 Administrative Guide (*July 2012*)
2. CA Arcot-WebFort-7.0 Administrative Guide *(June 2012)*