



# VCU Procurement Services

Date: July 1, 2021

Fischer International Identity  
9045 Strada Stell Court, Suite 201  
Naples, FL 34109

**Procurement Services**  
University Purchasing

912 W Grace Street, 5<sup>th</sup> Floor  
Box 980327  
Richmond, Virginia 23284

804 828-1077  
Fax: 804 828-7837  
TDD: 1-800-828-1120  
[www.vcu.edu/procurement](http://www.vcu.edu/procurement)

RE: Contract #: 7216216JC  
Renewal No. Four (4) of Four (4)

Dear Mr. Dagnall,

Your firm's contract with Virginia Commonwealth University (VCU) for Identity and Access Management Software and Services expires on July 17, 2021. VCU intends to exercise the renewal of this contract in accordance with the renewal terms of Contract # 7216216JC.

Your signature constitutes your firm's acceptance of this renewal, to include the optional use language.

## **OPTIONAL USE CONTRACT:**

This contract is an optional use, requirements based contract. VCU is in no way required to make purchases from the Contractor and may, in its sole discretion, purchase the identical and/or similar goods/services from other sources. Services shall be provided in accordance with the contract for the renewal period: July 18, 2021 through July 17, 2022.

Pricing remains the same as the previous contract period.

Attached is the revised pricing in accordance with the contract terms.

By signing and submitting this contract renewal letter Contractor certifies that it will maintain the insurance coverages required at the time the contract was awarded. At renewal, Contractor shall have a new Certificate of Insurance listing VCU as the "Additional Insured", citing the contractor's name and contract number, mailed to VCU Risk Management, Box 843040, Richmond, VA.

Please return this document to me no later than July 12, 2021. Your response may be emailed to me at [aranthes@vcu.edu](mailto:aranthes@vcu.edu). If you have any questions, please contact me at (804) 828-1070.

Sincerely,

Amy Anthes  
Category Manager

Contract #: 7216216JC

**RESPONSE:**

**Fischer International Identity LLC**

**Name of Firm**

DocuSigned by:  
*Dan Dagnall*

4FE26C008DF0465...  
**Signature**

**Daniel Dagnall**

**Name Printed**

**President & CEO**

**Title**

**July 12, 2021**

**Date**



**FISCHER IDENTITY**

Fischer International Identity, LLC  
 9045 Strada Stell Ct., Suite 201  
 Naples FL 34109  
 Tax ID # 20-5385349

**THIS IS NOT AN INVOICE**

# Renewal Order

<b>Date</b>	5/11/2021
<b>Order #</b>	SO-IDEN-1813
<b>Payment Terms</b>	Net 30
<b>Sales Rep</b>	Gary J O'Neill
<b>Contract #</b>	7216216JC
<b>PO #</b>	

**Bill To**  
 Virginia Commonwealth University  
 Accounts Payable  
 Box 3985  
 Scranton PA 18505-0985

**Ship To**  
 Virginia Commonwealth University  
 Attn: Mayura Patel  
 701 W Broad St  
 4th Floor  
 Richmond VA 23284

Description	Term Start	Term In Mo.	Term End	Rate	Amount
Fischer Identity Suite Annual Software License Maintenance Renewal	7/18/2021	12	7/17/2022		130,947.74

**Total** \$130,947.74

**All Prices are in US Dollars**

If you have questions about your order, please contact Gary J O'Neill at (678) 366-0426 or gary.o@fischeridentity.com.

Please submit Purchase Orders to Fischer.Acct@fischerinternational.com



# VCU Procurement Services

Date: June 22, 2020

Fischer International Identity  
9045 Strada Stell Court, Suite 201  
Naples, FL 34109

Procurement Services  
University Purchasing

912 W Grace Street, 5<sup>th</sup> Floor  
Box 980327  
Richmond, Virginia 23284

804 828-1077  
Fax: 804 828-7837  
TDD: 1-800-828-1120  
[www.vcu.edu/procurement](http://www.vcu.edu/procurement)

RE: Contract #: 7216216JC  
Renewal No. Three (3) of Four (4)  
Current Purchase Order: P0012225

Dear Mr. Sroka,

Your firm's contract with Virginia Commonwealth University (VCU) for Identity and Access Management Software and Services expires on July 17, 2020. VCU intends to exercise the renewal of this contract in accordance with the renewal terms of Contract # 7216216JC.

Your signature constitutes your firm's acceptance of this renewal, to include the optional use language and the eVA registration requirement provisions below.

### **OPTIONAL USE CONTRACT:**

This contract is an optional use, requirements based contract. VCU is in no way required to make purchases from the Contractor and may, in its sole discretion, purchase the identical and/or similar goods/services from other sources. Services shall be provided in accordance with the contract for the renewal period: July 18, 2020 through July 17, 2021.

- Pricing remains the same as the previous contract period.
- Attached is the revised pricing in accordance with the contract terms.
- By signing and submitting this contract renewal letter Contractor certifies that it will maintain the insurance coverages required at the time the contract was awarded. At renewal, Contractor shall have a new Certificate of Insurance listing VCU as the "Additional Insured", citing the contractor's name and contract number, mailed to VCU Risk Management, Box 843040, Richmond, VA.

Please return this document to me no later than June 30, 2020. Your response may be emailed to me at [aranthes@vcu.edu](mailto:aranthes@vcu.edu). If you have any questions, please contact me at (804) 828-1070.

Sincerely,

Amy Anthes  
Category Manager

Contract #: 7216216JC \_\_\_\_\_

**RESPONSE:**

**Fischer International Identity** \_\_\_\_\_

Name of Firm



Signature

**R. Andrew Sroka** \_\_\_\_\_

Name Printed

**President & CEO** \_\_\_\_\_

Title


**6/30/2020** \_\_\_\_\_

Date



# Status - PO P0053197

PO/Reference No. P0053197

Vendor Fischer International

General Information	Document Status
PO/Reference No. <b>P0053197</b>	Workflow  Completed (6/24/2020 8:59 AM)
Revision No. 0	Distribution The system distributed the purchase order using the method(s) indicated below the last time it was distributed: <a href="#">view</a>
Vendor Name Fischer International	Email (HTML Attachment): Fischer.Acct@fischerinternational.com
Purchase Order Date 6/24/2020	Distribution Date/Time 6/24/2020 8:59 AM
Total 129,651.23 USD	Vendor Sent To Vendor
Owner Name Tomekia James	Receiving none
Owner Phone +1 804-828-5870	Invoicing none
Owner Email tdjames@vcu.edu	Matching No Matches
Requisition Number 132180158	
A/P status Open	

## Line Item Status

	Product Description	Catalog No	Size / Packaging	Unit Price	Quantity	Ext. Price	Receiving	Invoicing	Matching
1 	Effective 7/18/2020 to 7/17/2021 (replaces EP2802252) Per Quote# SO-IDEN-1713 Fischer Identity SuiteAnnual Software License Maintenance Renewal 		EA	129,651.23 USD	1 EA	129,651.23 USD	none	none	No Matches

Shipping, Handling, and Tax charges are calculated and charged by each vendor. The values shown here are for estimation purposes, budget checking, and workflow approvals. Total **129,651.23 USD**



# VCU Procurement Services

Date: June 18, 2019

Fischer International Identity  
9045 Strada Stell Court, Suite 201  
Naples, FL 34109

RE: Contract #: 7216216JC  
Renewal No. Two  
Current Purchase Order: EP2763840

Procurement Services  
University Purchasing

912 W Grace Street, 5<sup>th</sup> Floor  
Box 980327  
Richmond, Virginia 23284

804 828-1077  
Fax: 804 828-7837  
TDD: 1-800-828-1120  
[www.vcu.edu/procurement](http://www.vcu.edu/procurement)

Dear Mr. O'Neill

Your firm's contract with Virginia Commonwealth University (VCU) for Identity and Access Management Software and Services expires on July 17, 2019. VCU intends to exercise the renewal of this contract in accordance with the renewal terms of contract # 7216216JC

Your signature constitutes your firm's acceptance of this renewal, to include the optional use language and the eVA registration requirement provisions below.

- Pricing remains the same as the previous contract period.  
 Attached is the revised pricing in accordance with the contract terms.
- By signing and submitting this contract renewal letter Contractor certifies that it will maintain the insurance coverages required at the time the contract was awarded. At renewal, Contractor shall have a new Certificate of Insurance listing VCU as the "Additional Insured", citing the contractor's name and contract number, mailed to VCU Risk Management, Box 843040, Richmond, VA.


Please return this document to me no later than July 1, 2019. Your response may be emailed to me at [aranthes@vcu.edu](mailto:aranthes@vcu.edu). If you have any questions, please contact me at (804) 828-1070.

Sincerely,  
Amy Anthes  
Category Manager

Contract #: 7216216JC

**RESPONSE:**

**Fischer International Identity**  
Name of Firm

Signature 

**R. Andrew Sroka**  
Name Printed

**President & CEO**  
Title

**June 20, 2019**  
Date





# VCU Procurement Services

Date June 14, 2018

Gary O'Neill  
9045 Strada Stell Court, Suite 201  
Naples, FL 34109

**Procurement Services**  
University Purchasing

912 W Grace Street, 5<sup>th</sup> Floor  
Box 980327  
Richmond, Virginia 23284

804 828-1077  
Fax: 804 828-7837  
TDD: 1-800-828-1120  
[www.vcu.edu/procurement](http://www.vcu.edu/procurement)

RE: Contract #: 7216216JC  
Renewal No.: One  
Current Purchase Order:

Dear Mr. O'Neill:

The current term for the Virginia Commonwealth University (VCU) Contract #7216216JC with Fischer International Identity expires on July 17, 2018. VCU intends to renew the contract from July 18, 2018 to July 17, 2019 in accordance with the renewal terms of the contract.

Your signature constitutes your firm's acceptance of this renewal, to include the optional use language and the eVA registration requirement provisions below.

This contract is an optional use contract. VCU is in no way required to make purchases from the Contractor and may in its sole discretion; purchase the identical and/or similar goods/services from other sources. Services shall be provided in accordance with the contract for the renewal period: July 18, 2018 through July 17, 2019.

- Pricing remains the same as the previous contract period.
- Attached is the revised pricing in accordance with the contract terms.
- By signing and submitting this contract renewal letter Contractor certifies that it will maintain the insurance coverages required at the time the contract was awarded. At renewal, Contractor shall have a new Certificate of Insurance listing VCU as the "Additional Insured", citing the contractor's name and contract number, mailed to VCU Risk Management, Box 843040, Richmond, VA.

Please return the completed and signed renewal document to me no later than June 22, 2018 by email to [pbanks3@vcu.edu](mailto:pbanks3@vcu.edu). If you have any questions, please contact me at (804) 828-0160.

Sincerely,

*Princess Banks*

Princess Banks  
Senior Buyer

**RESPONSE:**

Products and Services shall be provided in accordance with contract no. 7216216JC and this renewal form.

**Fischer International Identity**

Name of Firm

---

Signature

---

**R. Andrew Sroka**

Name Printed

---

**President & CEO**

Title

---

**June 18, 2018**

Date

---



THIS IS NOT AN INVOICE

# Renewal Order

Fischer International Identity, LLC  
9045 Strada Stell Ct., Suite 201  
Naples FL 34109  
Tax ID # 20-5385349

Date	5/9/2018
Order #	SO-IDEN-1499
Payment Terms	Net 30
Sales Rep	Gary J O'Neill
Contract #	7216216JC
PO #	

**Bill To**  
Virginia Commonwealth University  
Attn: AP  
912 W Grace St Fl 5  
Richmond VA 23284-9065

**Ship To**  
Virginia Commonwealth University  
701 W Broad St  
Richmond VA 23220-3804

Description	Term Start	Term In Mo.	Term End	Rate	Amount
Fischer Identity Suite Annual Software License Maintenance Renewal	7/18/2018	12	7/17/2019		129,651.23

**Total** \$129,651.23

**All Prices are in US Dollars**

If you have questions about your order, please contact Gary J O'Neill at (678) 366-0426 or [gjo@fischerinternational.com](mailto:gjo@fischerinternational.com).

Please submit Purchase Orders to [Fischer.Acct@fischerinternational.com](mailto:Fischer.Acct@fischerinternational.com)



# CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)  
6/19/2018

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

**IMPORTANT:** If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

<b>PRODUCER</b> Lassiter-Ware Insurance of Maitland 2701 Maitland Center Parkway Suite 125 Maitland FL 32751	<b>CONTACT NAME:</b> Rebekah Pickering <b>PHONE (A/C, No, Ext):</b> (800) 845-8437 <b>FAX (A/C, No):</b> (888) 883-8680 <b>E-MAIL ADDRESS:</b> BekahP@lassiter-ware.com																				
	<table border="1"> <thead> <tr> <th colspan="2">INSURER(S) AFFORDING COVERAGE</th> <th>NAIC #</th> </tr> </thead> <tbody> <tr> <td>INSURER A:</td> <td>Pacific Indemnity Company</td> <td>20346</td> </tr> <tr> <td>INSURER B:</td> <td>Federal Insurance Company</td> <td>20281</td> </tr> <tr> <td>INSURER C:</td> <td>AXIS Surplus Insurance Co.</td> <td>26620</td> </tr> <tr> <td>INSURER D:</td> <td></td> <td></td> </tr> <tr> <td>INSURER E:</td> <td></td> <td></td> </tr> <tr> <td>INSURER F:</td> <td></td> <td></td> </tr> </tbody> </table>	INSURER(S) AFFORDING COVERAGE		NAIC #	INSURER A:	Pacific Indemnity Company	20346	INSURER B:	Federal Insurance Company	20281	INSURER C:	AXIS Surplus Insurance Co.	26620	INSURER D:			INSURER E:			INSURER F:	
INSURER(S) AFFORDING COVERAGE		NAIC #																			
INSURER A:	Pacific Indemnity Company	20346																			
INSURER B:	Federal Insurance Company	20281																			
INSURER C:	AXIS Surplus Insurance Co.	26620																			
INSURER D:																					
INSURER E:																					
INSURER F:																					
<b>INSURED</b> Fischer International Identity, LLC et al  P O Box 9107 Naples FL 34101-9107																					

**COVERAGES**                      **CERTIFICATE NUMBER:** 18/19 FII MASTER                      **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	<input checked="" type="checkbox"/> COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR  GEN'L AGGREGATE LIMIT APPLIES PER: <input checked="" type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input type="checkbox"/> LOC OTHER:	X		35768315ECE	3/1/2018	3/1/2019	EACH OCCURRENCE \$ 1,000,000 DAMAGE TO RENTED PREMISES (Ea occurrence) \$ 1,000,000 MED EXP (Any one person) \$ 10,000 PERSONAL & ADV INJURY \$ 1,000,000 GENERAL AGGREGATE \$ 2,000,000 PRODUCTS - COMP/OP AGG \$ 2,000,000
B	<b>AUTOMOBILE LIABILITY</b> <input type="checkbox"/> ANY AUTO <input type="checkbox"/> ALL OWNED AUTOS <input type="checkbox"/> SCHEDULED AUTOS <input checked="" type="checkbox"/> HIRED AUTOS <input checked="" type="checkbox"/> NON-OWNED AUTOS			73508370	3/1/2018	3/1/2019	COMBINED SINGLE LIMIT (Ea accident) \$ 1,000,000 BODILY INJURY (Per person) \$ BODILY INJURY (Per accident) \$ PROPERTY DAMAGE (Per accident) \$
B	<input checked="" type="checkbox"/> UMBRELLA LIAB <input checked="" type="checkbox"/> OCCUR <input type="checkbox"/> EXCESS LIAB <input type="checkbox"/> CLAIMS-MADE DED    RETENTION \$			79794090	3/1/2018	3/1/2019	EACH OCCURRENCE \$ 10,000,000 AGGREGATE \$ 10,000,000
	<b>WORKERS COMPENSATION AND EMPLOYERS' LIABILITY</b> ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below		N/A				PER STATUTE    OTH-ER E.L. EACH ACCIDENT \$ E.L. DISEASE - EA EMPLOYEE \$ E.L. DISEASE - POLICY LIMIT \$
C	Tech & Prof Liab w/ Content Security & Privacy Liab			ECN000227161801	3/1/2018	3/1/2019	Each Wrongful Act \$2,000,000 Total Limit of Insurance \$2,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

Re: Contractor's Name: Fischer International Identity; Contract #7216216JC  
Virginia Commonwealth University is included as an additional insured under the terms and conditions of the general liability policy with respects to work being performed by the named insured as required by written contract.

<b>CERTIFICATE HOLDER</b>  Virginia Commonwealth University Contract #7216216JC Attention: VCU Risk Management Box 843040 Richmond, VA 23284	<b>CANCELLATION</b>  SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.  AUTHORIZED REPRESENTATIVE  Paul Ziccardi/KRISTT
--	--

© 1988-2014 ACORD CORPORATION. All rights reserved.

**COMMONWEALTH OF VIRGINIA  
STANDARD CONTRACT**

**Contract Number: 7216216JC**

This contract entered into by Fischer International Identity, LLC., hereinafter called the "Contractor" and Commonwealth of Virginia, Virginia Commonwealth University (VCU), called the "Purchasing Agency".

**WITNESSETH** that the Contractor and the Purchasing Agency, in consideration of the mutual covenants, promises and agreements herein contained, agree as follows:

**PERIOD OF THE PERFORMANCE:** From July 18, 2017 to July 17, 2018 with four (4) successive one year renewal options.

**SCOPE OF CONTRACT:** The Contractor shall provide the goods/services to the Purchasing Agency as set forth in the Contract Documents.

The contract documents shall consist of:


- (1) This signed form;
- (2) RFP #7216216JC dated October 17, 2016; Addendum #1 dated October 26, 2016 and Addendum #2 dated November 2, 2016;
- (3) The Contractor's Proposal dated November 9, 2016; and
- (4) The Negotiated Modifications dated June 21, 2017 and Negotiated Price dated July 6, 2017.

All of which documents are incorporated herein by reference.

IN WITNESS WHEREOF, the parties have caused this Contract to be duly executed intending to be bound thereby.

**CONTRACTOR:**

Fischer International Identity, LLC.

By: 

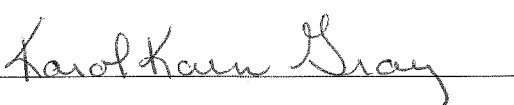
Name Printed: R. Andrew Sroka

Title: President & CEO

Date: 7-10-2017

**PURCHASING AGENCY:**

Virginia Commonwealth University

By: 

Name Printed: Karol Kain Gray

Title: Vice President for Finance and Budget

Date: 7-13-17



**VCU**

# Request for Proposals

RFP #: 7216216JC

RFP Title #: Identity and Access Management (IAM) Software and Services

Issuing Agency: Virginia Commonwealth University

Issue Date: October 17, 2016

Closing Date: November 17, 2016 at 11:00 AM



A VASCUPP Member Institution

**Request for Proposals RFP #7216216JC**

**Issue Date:** October 17, 2016  
**Title:** Identity and Access Management (IAM) Software and Services  
**Send all Proposals To:** Virginia Commonwealth University  
RFP #7216216JC  
Attention: Jackie Colbert  
912 W Grace St, 5th floor  
Richmond, Virginia 23284-0327

**Proposals Shall Be Received Until: November 17, 2016 at 11:00 AM local time**

**Direct ALL inquiries concerning this RFP to: Jackie Colbert**  
**jcolbert@vcu.edu**

**Questions concerning this RFP must be received via email no later than: October 26, 2016 at 3:00 PM local time.**

This Request for Proposals & any Addenda are posted on the eVA website at: <http://www.eva.virginia.gov>

HARD-COPY, ORIGINAL PROPOSALS MUST BE RECEIVED IN VIRGINIA COMMONWEALTH UNIVERSITY'S DEPARTMENT OF PROCUREMENT SERVICES ON OR BEFORE THE DATE AND TIME DESIGNATED ON THIS SOLICITATION. ELECTRONIC SUBMISSIONS AND FACSIMILE SUBMISSIONS WILL NOT BE ACCEPTED IN LIEU OF THE HARD-COPY, ORIGINAL PROPOSAL. VENDORS ARE RESPONSIBLE FOR THE DELIVERY OF THEIR PROPOSAL. PROPOSALS RECEIVED AFTER THE OFFICIAL DATE AND TIME WILL BE REJECTED. THE OFFICIAL DATE AND TIME USED IN RECEIPT OF RESPONSES IS THAT TIME ON THE CLOCK OR AUTOMATIC TIME STAMP IN THE DEPARTMENT OF PROCUREMENT SERVICES.

**IF PROPOSALS ARE HAND DELIVERED OR SENT BY FEDEX, UPS, OR ANY OTHER PRIVATE COURIER, DELIVER TO THE ADDRESS NOTED ABOVE. IF USING US MAIL (NOT RECOMMENDED): IF PROPOSALS ARE MAILED VIA US MAIL ONLY, MAIL TO VIRGINIA COMMONWEALTH UNIVERSITY, RFP#7216216JC, ATTN: Jackie Colbert, PO BOX 980327, RICHMOND, VA 23298-0327. THE RFP NUMBER, DATE AND TIME OF PROPOSAL SUBMISSION DEADLINE, AS REFLECTED ABOVE, MUST CLEARLY APPEAR ON THE FACE OF THE RETURNED PROPOSAL PACKAGE.**

In Compliance With This Request for Proposals And To All Conditions Imposed Therein and Hereby Incorporated By Reference, The Undersigned Offers And Agrees To Furnish The Goods/Services Described Herein In Accordance With The Attached Signed Proposal Or As Mutually Agreed Upon By Subsequent Negotiation. Furthermore, The Undersigned Agrees Not To Start Any Work Relative To This Particular Solicitation Until A Resulting Formal Signed Purchase Order Is Received By The Contractor From University's Department of Procurement Services. Any Work Relative To This Request for Proposals Performed By The Contractor Prior To Receiving A Formal Signed Purchase Order Shall Be At The Contractor's Own Risk And Shall Not Be Subject To Reimbursement By The University.

**Signature below constitutes acknowledgement of all information contained through links referenced herein.**

**NAME AND ADDRESS OF COMPANY:**

\_\_\_\_\_ Date: \_\_\_\_\_  
\_\_\_\_\_ By (Signature In Ink): \_\_\_\_\_  
\_\_\_\_\_ Zip Code \_\_\_\_\_ Name Typed: \_\_\_\_\_  
E-Mail Address: \_\_\_\_\_ Title: \_\_\_\_\_  
Telephone: ( \_\_\_\_ ) \_\_\_\_\_ Fax Number: ( \_\_\_\_ ) \_\_\_\_\_  
**Toll free, if available** **Toll free, if available**  
DUNS NO.: \_\_\_\_\_ FEI/FIN NO.: \_\_\_\_\_

REGISTERED WITH eVA: ( ) YES ( ) NO SMALL BUSINESS: ( ) YES ( ) NO  
VIRGINIA DSBSD CERTIFIED: ( ) YES ( ) NO MINORITY-OWNED: ( ) YES ( ) NO  
DSBSD CERTIFICATION #: \_\_\_\_\_ WOMEN-OWNED: ( ) YES ( ) NO

**A Pre-Proposal conference will be held. See Section IV herein for additional information.**

**THIS SOLICITATION CONTAINS 29 PAGES.**

## TABLE OF CONTENTS

	<b>PAGE</b>
I. <u>PURPOSE</u>	4
II. <u>GOVERNING RULES</u>	4
III. <u>BACKGROUND</u>	4
IV. <u>PRE-PROPOSAL CONFERENCE</u>	5
V. <u>STATEMENT OF NEEDS</u>	5
VI. <u>PROPOSAL PREPARATION AND SUBMISSION INSTRUCTIONS</u>	8
VII. <u>PRICING SCHEDULE</u>	11
VIII. <u>EVALUATION AND AWARD CRITERIA</u>	11
IX. <u>REPORTING AND DELIVERY INSTRUCTIONS</u>	11
X. <u>GERNERAL TERMS AND CONDITONS</u>	12
XI. <u>SPECIAL TERMS AND CONDITONS</u>	18
XII. <u>SPECIAL TERMS AND CONDITONS INFORMATION TECHNOLOGY</u>	22
XIII. <u>CONTRACT ADMINISTRATION</u>	28
XIV. <u>ATTACHMENTS</u>	29



## **I. PURPOSE:**

The intent and purpose of this Request for Proposals (RFP) is to establish a partnership with a qualified Identity and Access Management (IAM) vendor(s) for a software and services solution that meets the detailed requirements collected for VCU's IAM program.

It is the intent of this solicitation and resulting contract(s) to allow for cooperative procurement. Accordingly, any public body, public or private health or educational institution or lead-issuing institution's affiliated foundations may access any resulting contract(s) if authorized by the Contractor.

Participation in this cooperative procurement is strictly voluntary. If authorized by the Contractor(s), the resultant contract(s) may be extended to the entities indicated above to purchase at contract prices in accordance with contract terms. The Contractor shall notify the lead-issuing institution in writing of any entities accessing the contract. No modification of this contract or execution of a separate contract is required to participate. The Contractor shall provide usage reports for all entities accessing the Contract upon request. Participating entities shall place their own orders directly with the Contractor(s) and shall fully and independently administer their use of the contract(s) to include contractual disputes, invoicing and payments without direct administration from the lead-issuing institution. The lead-issuing institution shall not be held liable for any costs or damages incurred by any other participating entity as a result of any authorization by the Contractor to extend the contract. It is understood and agreed that the lead-issuing institution is not responsible for the acts or omissions of any entity, and will not be considered in default of the Agreement no matter the circumstances.

Use of this contract(s) does not preclude any participating entity from using other contracts or competitive processes.

## **II. GOVERNNG RULES:**

This solicitations is issued in accordance with the provisions of:

- A. Purchasing Manual for Institution of Higher Education and their Vendors (<https://vascupp.org>)
- B. Rules Governing Procurement of goods, Services, Insurance, and Construction by a Public Institution of Higher Education of the Commonwealth of Virginia (<https://vascupp.org>)

## **III. BACKGROUND:**

The University is located on two downtown Campuses in Richmond, VCU enrolls more than 32,000 students in 211 certificate and degree programs in the arts, sciences and humanities. Sixty-nine of the programs are unique in Virginia, many of them crossing the disciplines of VCU's 14 degree-granting schools and one college. As one of the nation's top research universities, VCU attracts more than \$225 million a year in sponsored research funding.

Twenty-seven VCU graduate and professional programs are ranked among the best in the nation in U.S. News & World Report's "America's Best Graduate Schools." These include the No. 1 ranked sculpture and nurse anesthesia programs.

VCU Life Sciences has developed into a University-wide discipline that builds upon the University's traditional scientific strengths in the biological sciences, basic biomedical sciences, patient care, biomedical engineering and biotechnology. VCU Life Sciences is comprehensive in its involvement of all levels of students in the study of life sciences, from freshmen to students in the professional programs to Ph.D. candidates, and integrates diverse disciplines from all over the University, including the academic medical center as well as arts and humanities.

VCU Medical Center is one of the nation's leading academic medical centers and stands alone as the only academic medical center in Central Virginia. The medical center includes the 780-bed MCV Hospitals and outpatient clinics, MCV Physicians — a 600-physician-faculty group practice, and the health sciences schools of VCU. The VCU Medical Center offers state-of-the art care in more than 200 specialty areas, many of national and international note, including organ transplantation, head and spinal cord trauma, burn healing and cancer treatment. The VCU Medical Center is the site for the region's only Level 1 Trauma Center. As a leader in health care research, the VCU Medical Center offers patients the opportunity to choose to participate in programs that advance evolving treatment, such as those sponsored by the National Cancer Institute through VCU's Massey Cancer Center, Virginia's first NCI-designated cancer center.

VCU's nationally recognized theatre, music and dance programs offer more than 365 concerts, performances and recitals a year. The Anderson Gallery showcases regional art as well as work by international artists.

VCU is an urban leader, forging ties with business, industry and government in such innovative projects as the collocation of the schools of Business and Engineering, the da Vinci Center for Innovation in Product Design and Development and the Virginia BioTechnology Research Park.

The University and its medical center are the largest-single employer in the Richmond area, with more than 12,000 full-time and 6,000 part-time employees, including 1,900 full-time instructional faculty — many of them nationally and internationally recognized in their fields. John B. Fenn, Ph.D., research professor in the Department of Chemistry and affiliate professor of chemical engineering, was one of three international scientists to be awarded the 2002 Nobel Prize in chemistry.

#### **IV. PRE-PROPOSAL CONFERENCE:**

An optional pre-proposal conference will be held at 2:00 PM on October 31, 2016 at:

VCU Technology Services  
Technology Administration Building (TAB)  
701 West Broad Street  
Room 202  
Richmond, Virginia 23220

Note: – Offerors should submit questions about the RFP via email by October 26, 2016 at 2:00 PM local time to [jcolbert@vcu.edu](mailto:jcolbert@vcu.edu).

The purpose of the conference is to allow Offerors an opportunity to ask questions and obtain clarification relative to any facet of this solicitation.

While attendance at this conference is optional, Offerors who intend to submit a proposal are highly encouraged to attend and to have a copy of this solicitation to reference. Any questions and answers that are presented during the conference or any changes to the solicitation resulting from this conference will be issued in a written addendum to the solicitation.

#### **V. STATEMENT OF NEEDS:**

The Identity & Access Management (IAM) program in the VCU Technology Services organization is working on an effort to design, develop, and build a centrally managed system of foundational core information security technology services. There are several releases planned for the IAM Program focused on providing the right people with the right access to the right resource at the right time to provide services to students, faculty, staff, and affiliates, as well as protect VCU's information and physical assets.

The tables below highlight relevant key information, applications, systems, and technologies at VCU.

Key Information	Quantity
Number of Employees(Classified & Faculty)	<ul style="list-style-type: none"> <li>• 6,000 full-time employees</li> <li>• 5,500 part-time employees</li> </ul>
Faculty	<ul style="list-style-type: none"> <li>• 2,264 full-time faculty</li> <li>• 1,015 part-time faculty</li> </ul>
Affiliates	<ul style="list-style-type: none"> <li>• ~10,000</li> </ul>
Total Number of Active Students	<ul style="list-style-type: none"> <li>• ~32,000</li> </ul>
Alumni	<ul style="list-style-type: none"> <li>• ~ 174,573</li> </ul>

Key Applications and Systems	Details
Banner	Enterprise Resource Planning (ERP) platform for human resources, finance, admissions, etc.
Google Apps for Education	Email, calendaring, Hangouts and collaboration
Office 365	Office 365 Education
CBORD	Physical access control and University card ("VCU CARD")
C-CURE	Physical access control and University card ("VCU CARD")
Blackboard	Cloud - Ver 9.1 - Rel 2015 Q4
NetIQ eDirectory	Version 8.8.8
Active Directory	Functional Level 2008 R2 (on Windows 2012r2)
Operating Systems (Servers)	Windows 2008 R2, Windows Server 2012 R2, RHEL 5,6, 7
Operating Systems (Desktop)	Windows 7, 8, 8.1, 10, OS X
Single Sign-on	CAS 3.5.3
Federation	Shibboleth IDP 3 ADFS 2012 R2
Service Request	LANDESK Service Desk

Management	
Databases	Microsoft SQL Server, MySQL, Oracle
Application Servers	IIS, WebLogic, WebSphere, Tomcat
Midrange	None
Mainframe	None
Virtual Desktop Infrastructure	Citrix

**A. Key IAM Program Deliverables**

1. Deliver "birthright" provisioning and automated de-provisioning of key applications, such as Google Apps for Work, Banner, Active Directory, NetIQ eDirectory and physical / badge access.
2. Simplify and improve the operations and support of provisioning and de-provisioning activities (constraint = inexpensive to support IAM development/infra)
3. Provide visibility into who has access to what, so that VCU can take actions to improve access administration, simplify rules and policies, and improve its security posture.
4. Deliver password self-service function to employees, contractors, students, and faculty.

**B. Detailed Requirements**

Attached is Schedule A, which details requirements relevant for this RFP. Please note four (4) tabs in Schedule A.

1. Technology Requirements - the first tab is focused on the technical capabilities of the proposed software solution.
2. Professional Services - the second tab is specific to the services portion of the RFP and roughly outlines the initial scope of the preferred implementation.
3. Pricing - the third tab is specific to the pricing of the proposals.
4. Security of Data - the fourth tab are the security requirements for the protection of data.

Please make sure to place all the responses for the schedule directly into the Excel spreadsheet, unless otherwise noted. If additional supporting material is requested or provided please reference the corresponding question from the exhibit by Section and/or number. Any external materials will be treated as exhibits to the primary proposal so please make sure to follow this template carefully.

**C. Procurement Requirements:**

1. Freight terms shall be F.O.B. Destination/Prepaid with inside delivery; additional charges shall not be allowed.
2. The terms and conditions of the RFP govern the resulting contract and not any Contractor terms and conditions or software license agreement.
3. The proposal prices shall include all costs for the equipment and services including all applicable freight and travel and living expenses; extra charges will not be allowed.
4. The initial contract term is one (1) year with four (4) annual, optional renewal terms.
5. VCU reserves the right to made separate awards for the technology requirements and the professional services.

6. Upon award of the contract, VCU anticipates the service provider should develop the Statement of Work (SOW) based on the agreed upon terms in the contract to include all business requirements.

## **VI. PROPOSAL PREPARATION AND SUBMISSION INSTRUCTIONS:**

### A. Proposal Submission Instructions:

1. Complete and return Page 2 of the RFP. Proposals shall be signed by an authorized representative of the Offeror.
2. Complete and return signed addenda acknowledgments (if applicable).
3. Submit **one (1) original hard copy (paper)** of the entire proposal, including all attachments and proprietary information. The original proposal must be clearly marked on the outside of the proposal. Submit one (1) unsecured, electronic copy (on a disc or flash drive) of the entire proposal including all attachments and **INCLUDING ANY PROPRIETARY INFORMATION** and one (1) unsecured, electronic copy (on a disc or flash drive) of the entire proposal including all attachments and **EXCLUDING ANY PROPRIETARY INFORMATION**. These discs or flash drives must be clearly marked on the outside whether it includes or excludes proprietary information. The copies of the RFP in this Section are for Procurement Services.
4. Submit two (2) hard copies (paper copies) of the entire proposal, **INCLUDING ALL ATTACHMENTS AND ANY PROPRIETARY INFORMATION** and **ten (10) unsecured electronic copies** (on a disc or flash drive) of the **entire** proposal, **INCLUDING ALL ATTACHMENTS AND ANY PROPRIETARY INFORMATION** for the Evaluation Committee Members.
5. Proposal Presentation:
  - a. All information requested must be submitted. Failure to submit all information requested may result in the Purchasing Agency requiring prompt submission of missing information and/or giving a lowered evaluation of the proposal. Proposals which are substantially incomplete or lack key information may be rejected by the purchasing agency. Mandatory requirements are those required by law or regulation or are such that they cannot be waived and are not subject to negotiation.
  - b. All information requested by this Request for Proposals on the ownership, utilization and planned involvement of small businesses, women-owned businesses and minority-owned businesses must be submitted. If an Offeror fails to submit all information requested, the Purchasing Agency may require prompt submission of missing information after the receipt of Contractors proposals.
  - c. Proposals should be prepared simply and economically, providing a straightforward, concise description of capabilities to satisfy the requirements of the RFP. Emphasis should be placed on completeness and clarity of content.
  - d. Proposals should be organized as specified in the RFP. All pages of the proposal should be numbered. The proposal should contain a table of contents, which cross-references the RFP requirements. Information which the offeror desires to present that does not fall within any of the requirements of the RFP should be inserted at an appropriate place or be attached at the end of the proposal and designated as additional material. Proposals that are not organized in this manner risk elimination from consideration if the evaluators are unable to find the RFP requirements are specifically addressed.
  - e. Each copy of the proposal should be bound or contained in a single volume where practical. All documentation submitted with the proposal should be contained in that single volume.
6. If applicable, the outside of the Proposal must be marked to clearly denote proprietary information is contained in the documents. **Written notice of proprietary information must be submitted as the first page of the Offeror's Proposal.** Notice must specifically identify the applicable portions of the Offeror's Proposal that contain data or materials to be protected and

shall state the reasons why protection is necessary. In addition, the specific (i.e. specific words, figures or paragraphs) proprietary or trade secret material submitted must be identified on the applicable page(s) within the Offeror's Proposal, by some distinct method, such as highlighting, underlining, etc. The classification of an entire Proposal document, line item prices and/or total Proposal prices as proprietary or trade secrets is not acceptable and may result in rejection and return of the Proposal. Ownership of all data, materials and documentation originated and prepared for VCU pursuant to the RFP shall belong exclusively to the University and be subject to public inspection in accordance with the Virginia Freedom of Information Act. Trade secrets or proprietary information submitted by an Offeror shall not be subject to public disclosure under the Virginia Freedom of Information Act; however, the Offeror must invoke the protections of Section 43F of The Governing Rules, in writing, either before or at the time the data or other material is submitted.

7. Communications regarding this Request for Proposals (RFP) shall be formal from the date of the issuance for this RFP, until either a Contractor has been selected or the University Procurement Services Department rejects all proposals. Formal communications shall be directed to the University Procurement Department only. Informal communications including but not limited to, request for information, comments or speculations, regarding this RFP to any University employee other than Procurement Services Department representative may result in the offending Offeror's Proposal being rejected.
8. Oral Presentation: Offerors who submit a proposal in response to this RFP may be required to conduct an oral presentation of their proposal to VCU. Oral presentations are an option and may or may not be required. Should an oral presentation be required, VCU will designate the date and location for the presentation; the date is critical and alternative dates will not be available. Offerors who are invited to conduct an oral presentation shall include the individual(s) who would be the primary point of contact for VCU, on the Offerors presentation team.
8. The version of the solicitation issued by the Virginia Commonwealth University Purchasing Department as amended by any addenda is the mandatory controlling version of the document. Any modification of or additions to the solicitation by the Offeror shall not modify the official version of the solicitation issued by the Virginia Commonwealth University Purchasing Department unless accepted in writing by the University. Such modifications or additions to the solicitation by the Offeror may be cause for rejection of the proposal; however, Virginia Commonwealth University reserves the right to decide, on a case by case basis, in its sole discretion, whether to reject such a proposal. If the modifications or additions are not identified until after the award of the contract, the controlling version of the solicitation document shall still be the official state form issued by the Purchasing Department.

B. Specific Proposal Requirements:

1. Proposals should be as thorough and detailed as possible so that VCU may properly evaluate your capabilities to provide the required goods/services.
2. Proposed Price.
  - a. Complete the third tab of Schedule A with the requested pricing information. Schedule A must contain all costs for the proposed IAM solution. Additional charges shall not be allowed.
3. Complete the first, second and fourth tab of Schedule A to provide specific plans and approach for providing the proposed software and services for the IAM solution proposed. **Mandatory requirements are designated by the words shall or must and desirable services are designated by the words should or may.**
4. Does / Shall your company agree to comply with all of the Procurement Requirements in Section V.C.?
5. Utilization of the words "shall" or "must" in Schedule A and Section V., Statement of Needs indicates a mandatory requirement:

Does / Shall your company comply with mandatory requirements as presented in Schedule A and Section V., Statement of Needs?

Yes \_\_\_\_ No \_\_\_\_

If "NO," identify the specific requirement and the reason for non-compliance.

6. Utilization of the words "should" or "may" in Section V, Statement of Needs indicates a non-mandatory requirement.

Does / Shall your company comply the non-mandatory requirements as presented in Schedule A and Section V., Statement of Needs (i.e. "should" becomes "shall")?

Yes \_\_\_\_ No \_\_\_\_

If "NO," identify the specific requirement and the reason for non-compliance.

7. Submit information about the qualifications and experience that your company has to provide the required products and services.

- a. Describe the firm's qualifications and experience providing the required products and services during the last three (3) years. Information provided should include, but is not limited to, comparable accounts in higher education and the scope of the services. Include information for a minimum of three (3) similar accounts, describing the types of projects and the scope of the services provided. Please include contact information with the name, address, email address and current phone number.
- b. Specify any technicians your company intends to assign to the VASCUPP contract. Provide information to include but is not limited to the names, qualifications, and experience of the technicians to be assigned to the contract. Resumes of staff to be assigned to the contract may be used. Submit relevant professional certifications for the technicians proposed to work on contract projects.
- c. Does the offer include a single primary point of contact for the VASCUPP institutions for sales, support and problem resolution? If so, please provide the name and contact information.
- d. Provide a list of institutions of higher education with which your firm has a signed term contract.
- e. Provide the amount of annual sales the firm has with each VASCUPP Member Institution. A list of VASCUPP Members can be found at:

<http://procurement.vcu.edu/our-services/university-purchasing/vascupp/>

8. Does your company accept the terms and conditions as presented in Section X, General Terms and Conditions and in Section XI, Special Terms and Conditions to govern the contract?

Yes \_\_\_\_ No \_\_\_\_

If "NO," identify the specific term and condition(s) and the reason for non-compliance.

10. Small, Women-Owned and Minority-Owned Business commitment for utilization.

- a. The Offeror must submit complete information on Appendix I unless the Offeror is a Department of Small Business and Supplier Diversity (DSBSD). DSBSD certified small businesses must include their certification number on the coversheet of this RFP, but are not required to complete Appendix I.

11. Method of Payment

- a. The Offeror must complete and submit Appendix II to select an electronic payment method.

## **VII. PRICING SCHEDULE:**

Tab 3 – Pricing of Schedule A will be used during the RFP evaluation process to determine the scores for the price evaluation criterion. In the event of a mathematical error, the correct unit price shall prevail. The proposal prices shall include all costs for the products and services including all applicable freight and travel and living expenses; extra charges will not be allowed. Complete the third tab of Schedule A with the requested pricing information.

## **VIII. EVALUATION AND AWARD CRITERIA:**

Proposals will be evaluated based upon the information provided in the Offeror's Proposal using the following criteria: Offeror's qualifications and experience; methodology/approach to providing the requirements stated herein; price; and the Offeror's status as a Virginia certified SWaM Business or the Offeror's plans to utilize Virginia DSBSD certified SWaM Businesses in the Offeror's performance of the contract. Negotiations shall be conducted with Offerors so selected. After negotiations have been conducted with each Offeror so selected, the VCU shall select the Offeror which, in its opinion, has made the best offer, and shall award the contract to that Offeror. VCU reserves the right to make multiple awards from the RFP. The University may cancel this Request for Proposals or reject Proposals at any time prior to an award, and is not required to furnish a statement of the reason why a particular Proposal was not deemed to be the most advantageous. (Governing Rules Section 49.D) Should the University determine in writing and in its sole discretion that only one Offeror has made the best proposal, a Contract may be negotiated and awarded to that Offeror. The award document will be a Contract incorporating by reference all the requirements, terms and conditions of the RFP, and the Offeror's response thereto.

Notice of Award(s) or Notice of Intent to Award may be accessed electronically at <http://www.eva.virginia.gov>.

## **IX. REPORTING AND DELIVERY REQUIREMENTS:**

**By submitting a Proposal, Offerors certify that all information provided in response to the Request for Proposals is true and accurate. Failure to provide information required by this Request for Proposals will ultimately result in rejection of the Proposal.**

It is the policy of the Commonwealth of Virginia that 42% of its purchases be made from small businesses to contribute to the establishment, preservation, and strengthening of small businesses, and businesses owned by women and minorities, and to encourage their participation in VCU procurement activities. The University encourages Contractors to provide for the participation of small businesses and businesses owned by women and minorities through partnerships, joint ventures, subcontracts or other contractual opportunities.

**Use of Subcontractors:** If the Offeror intends to use subcontractors to perform any portion of the work described in this RFP, the Offeror must clearly so state. VCU is placing an increased emphasis on its SWaM (Small, Women, and Minority Owned) business program and is interested in identifying any potential opportunities that may be available to engage SWaM vendors to be certified by the Virginia Department of Small Business and Supplier Diversity (DSBSD) through new or existing contracts. **Identify and list any such opportunities that your firm would commit to if awarded this Contract in Appendix I- Participation in VCU Procurement Transactions Small Businesses and Businesses Owned by Women and Minority.** The Offeror's response must include a description of which portion(s) of the work will be sub-contracted out and the names and addresses of potential Subcontractor(s) under the Contract.



**REPORT ON THE PARTICIPATION OF SMALL BUSINESSES AND BUSINESSES  
OWNED  
BY WOMEN AND MINORITIES**

Unless the Contractor is a DSBSD certified small business, the Contractor shall submit quarterly reports on the direct involvement of Department of Small Business and Supplier Diversity (DSBSD) certified SWaM Businesses in the performance of the Contract. The report shall specify the actual dollars spent to date with Small Businesses, Women-Owned Businesses, and Minority-Owned Businesses based upon the Contractor's commitment for utilization of DSBSD SWaM Businesses.

The Contractor shall provide this information to:

Virginia Commonwealth University  
Procurement Services Office  
Attn: SWAM Coordinator  
912 W. Grace Street, POB 980327  
Richmond, VA 23284  
Email: [swamreporting@vcu.edu](mailto:swamreporting@vcu.edu)

Failure to submit the required information will be considered a contract compliance issue and will be addressed accordingly. In addition, failure to submit the required information will result in invoices being returned without payment.

**X. GENERAL TERMS AND CONDITIONS:**

- A. PURCHASING MANUAL: This RFP is subject to the provisions of the Commonwealth of Virginia's Purchasing Manual for Institutions of Higher Education and their Vendors and any revisions thereto, which are hereby incorporated into this contract in their entirety. A copy of the manual is available for review at the VCU Procurement Services Office. In addition, the manual may be accessed electronically at <http://procurement.vcu.edu/> or a copy can be obtained by calling VCU Procurement Services at (804) 828-1077.
- B. APPLICABLE LAW AND COURTS: This RFP and any resulting Contract shall be governed in all respects by the laws of the Commonwealth of Virginia and any litigation with respect thereto shall be brought in the courts of the Commonwealth. The Contractor shall comply with all applicable federal, state and local laws, rules and regulations.
- C. ANTI-DISCRIMINATION: By submitting their Proposals, Offerors certify to the Commonwealth and to VCU that they will conform to the provisions of the Federal Civil Rights Act of 1964, as amended, as well as the Virginia Fair Employment Contracting Act of 1975, as amended, where applicable, the Virginians With Disabilities Act, the Americans With Disabilities Act and Section 2.2-4311 of the *Virginia Public Procurement Act*. If the award is made to a faith-based organization, the organization shall not discriminate against any recipient of goods, services, or disbursements made pursuant to the contract on the basis of the recipient's religion, religious belief, refusal to participate in a religious practice, or on the basis of race, age, color, gender or national origin and shall be subject to the same rules as other organizations that contract with public bodies to account for the use of the funds provided; however, if the faith-based organization segregates public funds into separate accounts, only the accounts and programs funded with public funds shall be subject to audit by the public body. (*Code of Virginia, § 2.2-4343.1*).

In every Contract over \$10,000 the provisions in 1. and 2. below apply:

1. During the performance of this Contract, the Contractor agrees as follows:

- a) Virginia Commonwealth University is an equal opportunity/affirmative action institution providing access to education and employment without regard to age, race, color, national origin, gender, religion, sexual orientation, veteran's status, political affiliation or disability. As such, the Contractor will not discriminate against any employee or applicant for employment because of age, race, color, national origin, gender, religion, sexual orientation, veteran's status, political affiliation or disability or any other basis prohibited by state law related to discrimination in employment, except where there is a bona fide occupational qualification reasonably necessary to the normal operation of the Contractor. The Contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices setting forth the provisions of this nondiscrimination clause.
  - b) The Contractor, in all solicitations or advertisements for employees placed by or on behalf of the Contractor, will state that such Contractor is an equal opportunity employer.
  - c) Notices, advertisements and solicitations placed in accordance with federal law, rule or regulation shall be deemed sufficient for the purpose of meeting these requirements.
2. The Contractor will include the provisions of 1. above in every subcontract or purchase order over \$10,000, so that the provisions will be binding upon each subcontractor or vendor.
- D. ETHICS IN PUBLIC CONTRACTING: By submitting their Proposals, Offerors certify that their Proposals are made without collusion or fraud and that they have not offered or received any kickbacks or inducements from any other Offeror, supplier, manufacturer or subcontractor in connection with their Proposal, and that they have not conferred on any public employee having official responsibility for this procurement transaction any payment, loan, subscription, advance, deposit of money, services or anything of more than nominal value, present or promised, unless consideration of substantially equal or greater value was exchanged.
- E. IMMIGRATION REFORM AND CONTROL ACT OF 1986: By submitting their Proposals, Offerors certify that they do not and will not during the performance of this Contract employ illegal alien workers or otherwise violate the provisions of the Federal Immigration Reform and Control Act of 1986.
- F. DEBARMENT STATUS: By submitting their Proposals, Offerors certify that they are not currently debarred by the Commonwealth of Virginia from submitting proposals on contracts for the type of goods and/or services covered by this solicitation, nor are they an agent of any person or entity that is currently so debarred.
- G. ANTITRUST: By entering into a Contract, the Contractor conveys, sells, assigns, and transfers to the Commonwealth of Virginia all rights, title and interest in and to all causes of the action it may now have or hereafter acquire under the antitrust laws of the United States and the Commonwealth of Virginia, relating to the particular goods or services purchased or acquired by the Commonwealth of Virginia under said contract.
- H. MANDATORY USE OF STATE FORM AND TERMS AND CONDITIONS: Failure to submit a Proposal on the official VCU Form provided for that purpose may be a cause for rejection of the Proposal. Modification of, or additions to, the General Terms and Conditions of the solicitation may be cause for rejection of the Proposal; however, the Commonwealth reserves the right to decide, on a case by case basis, in its sole discretion, whether to reject such a Proposal.

I. FINAL OF TERMS: If any prospective Offeror has questions about the specifications or other RFP documents, the prospective Offeror should contact the Services Category Manager whose name appears on the face of the RFP no later than five (5) working days before the Proposal due date. Any revisions to the RFP will be made only by Addendum issued by the Services Category Manager.

J. PAYMENT:

1. To Prime Contractor:

- a) Invoices for items ordered, delivered and accepted shall be submitted by the Contractor directly to the payment address shown on the purchase order/Contract. All invoices shall show the VCU Contract number and/or purchase order number; social security number (for individual Contractors) or the federal employer identification number (for proprietorships, partnerships, and corporations).
- b) Any payment terms requiring payment in less than thirty (30) days will be regarded as requiring payment thirty (30) days after invoice or delivery, whichever occurs last. This shall not affect offers of discounts for payment in less than thirty (30) days, however.
- c) All goods or services provided under this Contract or purchase order, that are to be paid for with public funds, shall be billed by the Contractor at the contract price, regardless of which public institution is being billed.
- d) The following shall be deemed to be the date of payment: the date of postmark in all cases where payment is made by mail, or the date of offset when offset proceedings have been instituted as authorized under the Virginia Debt Collection Act.
- e) Unreasonable Charges. Under certain emergency procurements and for most time and material purchases, final job costs cannot be accurately determined at the time orders are placed. In such cases, contractors should be put on notice that final payment in full is contingent on a determination of reasonableness with respect to all invoiced charges. Charges which appear to be unreasonable will be researched and challenged, and that portion of the invoice held in abeyance until a settlement can be reached. Upon determining that invoiced charges are not reasonable, VCU shall promptly notify the contractor, in writing, as to those charges which it considers unreasonable and the basis for the determination. A Contractor may not institute legal action unless a settlement cannot be reached within thirty (30) days of notification. The provisions of this Section do not relieve VCU of its prompt payment obligations with respect to those charges that are not in dispute (Code of Virginia, § 2.2-4363).

f) To Subcontractors:

- a) Contractor awarded a contract under this RFP is hereby obligated:
  - i. To pay the Subcontractor(s) within seven (7) days of the Contractor's receipt of payment from VCU for the proportionate share of the payment received for work performed by the Subcontractor(s) under the contract; or
  - ii. To notify VCU and the Subcontractor(s), in writing, of the Contractor's intention to withhold payment and the reason.
- b) The Contractor is obligated to pay the Subcontractor(s) interest at the rate of one percent per month (unless otherwise provided under the terms of the contract) on all amounts owed by the Contractor that remain unpaid seven (7) days following receipt

of payment from VCU, except for amounts withheld as stated in 2. above. The date of mailing of any payment by U.S. Mail is deemed to be payment to the addressee. These provisions apply to each sub-tier Contractor performing under the primary contract. A Contractor's obligation to pay an interest charge to a Subcontractor may not be construed to be an obligation of VCU.

- K. PRECEDENCE OF TERMS: Paragraphs A-J of these General Terms and Conditions shall apply in all instances. In the event there is a conflict between any of the other General Terms and Conditions and any Special Terms and Conditions in this solicitation, the Special Terms and Conditions shall apply.
- L. QUALIFICATIONS OF OFFERORS: VCU may make such reasonable investigations as deemed proper and necessary to determine the ability of the Offeror to perform the services/furnish the goods and the Offeror shall furnish to VCU all such information and data for this purpose as may be requested. VCU reserves the right to inspect Offeror's physical facilities prior to award to satisfy questions regarding the Offeror's capabilities. VCU further reserves the right to reject any Proposal if the evidence submitted by, or investigations of, such Offeror fails to satisfy VCU that such Offeror is properly qualified to carry out the obligations of the Contract and to provide the services and/or furnish the goods contemplated therein.
- M. TESTING AND INSPECTION: VCU reserves the right to conduct any test/inspection it may deem advisable to assure goods and services conform to the specifications.
- N. ASSIGNMENT OF CONTRACT: A Contract shall not be assignable by the Contractor in whole or in part without the written consent of the VCU Director of Procurement Services.
- O. CHANGES TO THE CONTRACT: Changes can be made to the Contract in any one of the following ways:
1. The parties may agree in writing to modify the scope of the Contract. An increase or decrease in the price of the Contract resulting from such modification shall be agreed to by the parties as a part of their written agreement to modify the scope of the Contract.
  2. The VCU Procurement Services Department may order changes within the general scope of the Contract at any time by written notice to the Contractor. Changes within the scope of the contract include, but are not limited to, things such as services to be performed, the method of packing or shipment, and the place of delivery or installation. The Contractor shall comply with the notice upon receipt. The Contractor shall be compensated for any additional costs incurred as the result of such order and shall give VCU a credit for any savings. Said compensation shall be determined by one of the following methods:
    - a) By mutual agreement between the parties in writing; or
    - b) By agreeing upon a unit price or using a unit price set forth in the Contract, if the work to be done can be expressed in units, and the Contractor accounts for the number of units of work performed, subject to the VCU's right to audit the Contractor's records and/or to determine the correct number of units independently; or
    - c) By ordering the Contractor to proceed with the work and keep a record of all costs incurred and savings realized. A markup for overhead and profit may be allowed if provided by the Contract. The same markup shall be used for determining a decrease in price as the result of savings realized. The Contractor shall present VCU with all vouchers and records of expenses incurred and savings realized. VCU shall have the right to audit the records of the Contractor as it deems necessary to determine costs or savings. Any claim for an adjustment in price under this provision must be asserted by written notice to VCU within thirty (30) days from the date of receipt of the written

order from VCU. If the parties fail to agree on an amount of adjustment, the question of an increase or decrease in the Contract price or time for performance shall be resolved in accordance with the procedures for resolving disputes provided by the Disputes Clause of this Contract or, if there is none, in accordance with the disputes provisions of the Commonwealth of Virginia's Purchasing Manual for Institutions of Higher Education and Their Vendors. Neither the existence of a claim or a dispute resolution process, litigation or any other provision of this Contract shall excuse the Contractor from promptly complying with the changes ordered by the VCU Procurement Service Office or with the performance of the Contract generally.

- P. DEFAULT: In case of failure to deliver goods or services in accordance with the Contract terms and conditions, VCU after due oral or written notice, may procure them from other sources and hold the Contractor responsible for any resulting additional purchase and administrative costs. This remedy shall be in addition to any other remedies which VCU may have in law or equity.
- Q. USE OF BRAND NAMES: Unless otherwise provided in this RFP, the name of a certain brand, make or manufacturer does not restrict Offerors to the specific brand, make or manufacturer named, but conveys the general style, type, character, and quality of the article desired. Any article, which the public body, in its sole discretion, determines to be the equal of that specified, considering quality, workmanship, economy of operation, and suitability for the purpose intended, shall be accepted. The Offeror is responsible to clearly and specifically identify the product being offered and to provide sufficient descriptive literature, catalog cuts and technical detail to enable VCU to determine if the product offered meets the requirements of the solicitation. This is required even if offering the exact brand, make or manufacturer specified. Unless the Offeror clearly indicates in its proposal that the product offered is an "equal" product, such proposal will be considered to offer the brand name product referenced in the RFP.
- R. TRANSPORTATION AND PACKAGING: By submitting their Proposals, all Offerors certify and warrant that the price offered for FOB Destination includes only the actual freight rate costs at the lowest and best rate and is based upon the actual weight of the goods to be shipped. Except as otherwise specified herein, standard commercial packaging, packing and shipping containers shall be used. All shipping containers shall be legibly marked or labeled on the outside with purchase order number, commodity description, and quantity. Further, Offeror shall bear the risk of loss until the goods and equipment until VCU accepts Delivery of them.
- S. INSURANCE: By signing and submitting a Proposal under this RFP, the Offeror certifies that if awarded the Contract, it will have the following insurance coverages at the time the Contract is awarded. For construction contracts, if any Subcontractors are involved, the subcontractor will have workers' compensation insurance in accordance with §§ 2.2-4332 and 65.2-800 et seq. of the *Code of Virginia*. The Offeror further certifies that the Contractor and any Subcontractors will maintain these insurance coverages during the entire term of the Contract and that all insurance coverage will be provided by insurance companies authorized to sell insurance in Virginia by the Virginia State Corporation Commission.

Minimum Insurance Coverages and Limits Required for Most Contracts:

1. Worker's Compensation - Statutory requirements and benefits. Coverage is compulsory for employers of three or more employees, to include the employer. Contractors who fail to notify VCU of increases in the number of employees that change their workers' compensation requirements under the *Code of Virginia* during the course of the Contract shall be in noncompliance with the Contract.
2. Employers Liability - \$100,000.

3. Commercial General Liability - \$1,000,000 per occurrence. Commercial General Liability is to include bodily injury and property damage, personal injury and advertising injury, products and completed operations coverage. VCU must be named as an additional insured and so endorsed on the policy.
4. Automobile Liability - \$1,000,000 per occurrence. (Only used if motor vehicle is to be used in the contract.)

T. ANNOUNCEMENT OF AWARD: Upon the award or the announcement of the decision to award a contract as a result of this RFP, VCU will publicly post such notice electronically at <http://www.eva.virginia.gov> for a minimum of ten (10) days.

U. DRUG-FREE WORKPLACE: During the performance of this Contract, the Contractor agrees to (i) provide a drug-free workplace for the Contractor's employees; (ii) post in conspicuous places, available to employees and applicants for employment, a statement notifying employees that the unlawful manufacture, sale, distribution, dispensation, possession, or use of a controlled substance or marijuana is prohibited in the contractor's workplace and specifying the actions that will be taken against employees for violation of such prohibition; (iii) state in all solicitations or advertisements for employees placed by or on behalf of the Contractor that the Contractor maintains a drug-free workplace; and (iv) include the provisions of the foregoing clauses in every Subcontract or purchase order of over \$10,000, so that the provisions will be binding upon each Subcontractor and/ or Vendor.

For the purposes of this section, "*drug-free workplace*" means a site for the performance of work done in connection with a specific Contract awarded to a Contractor, the employees of whom are prohibited from engaging in the unlawful manufacture, sale, distribution, dispensation, possession or use of any controlled substance or marijuana during the performance of the Contract.

V. NONDISCRIMINATION OF CONTRACTORS: A Bidder, Offeror, or Contractor shall not be discriminated against in the solicitation or award of this Contract because of race, religion, color, sex, national origin, age, disability, or against faith-based organizations or any other basis prohibited by state law relating to discrimination in employment. If the award of this Contract is made to a faith-based organization and an individual, who applies for or receives goods, services, or disbursements provided pursuant to this Contract objects to the religious character of the faith-based organization from which the individual receives or would receive the goods, services, or disbursements, the public body shall offer the individual, within a reasonable period of time after the date of his objection, access to equivalent goods, services, or disbursements from an alternative provider.

W. eVA BUSINESS-TO-GOVERNMENT VENDOR REGISTRATION, CONTRACTS, AND ORDERS: The eVA Internet electronic procurement solution, website portal [www.eVA.virginia.gov](http://www.eVA.virginia.gov), streamlines and automates government purchasing activities in VCU. The eVA portal is the gateway for vendors to conduct business with VCU Institution and other public bodies. All Vendors desiring to provide goods and/or services to VCU shall participate in the eVA Internet e-procurement solution by completing the free eVA Vendor Registration. All Bidders or Offerors must register in eVA and pay the Vendor Transaction Fees specified below; failure to register will result in the bid/proposal being rejected.

Vendor Transaction Fees are determined by the date the original purchase order is issued and are as follows:

1. For orders issued July 1, 2014 and after, the Vendor Transaction Fee is:
  - a) DSBSD-certified Small Businesses: 1%, capped at \$500 per order.

- b) Businesses that are not DSBSD-certified Small Businesses: 1%, capped at \$1,500 per order.
2. For orders issued July 1, 2014 the vendor transaction fees can be found at [www.eVA.virginia.gov](http://www.eVA.virginia.gov)

The specified vendor transaction fee will be invoiced, by the Commonwealth of Virginia Department of General Services, approximately thirty (30) days after the corresponding purchase order is issued and payable thirty (30) days after the invoice date. Any adjustments (increases/decreases) will be handled through purchase order changes.

- X. FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA). The Selected Offeror/Vendor acknowledges that for the purposes of this Contract it will be designated as a “school official” with “legitimate educational interests” in the University education records, as those terms have been defined under FERPA and its implementing regulations, and the Selected Firm/Vendor agrees to abide by the limitations and requirements imposed on school officials. Selected Firm/Vendor will use the education records only for the purpose of fulfilling its duties under this Contract for University’s and its students’ benefit, and will not share such data with or disclose it to any third party except as provided for in this Contract, required by law, or authorized in writing by the University.

#### **XI. SPECIAL TERMS AND CONDITIONS:**

- A. ADVERTISING: In the event a contract is awarded for supplies, equipment, or services resulting from this proposal, no indication of such sales or services to Virginia Commonwealth University will be used in product literature or advertising. The Contractor shall not state in any of the advertising or product literature that the Commonwealth of Virginia or any agency or institution of the Commonwealth has purchased or uses its products or services.
- B. AUDIT: The Contractor shall retain all books, records, and other documents relative to this contract for five (5) years after final payment, or until audited by the Commonwealth of Virginia, whichever is sooner. The agency, its authorized agents, and/or State auditors shall have full access to and the right to examine any of said materials during said period.
- C. AVAILABILITY OF FUNDS: It is understood and agreed between the parties herein that the agency shall be bound hereunder only to the extent of the funds available or which may hereafter become available for the purpose of this agreement.
- D. PROPOSAL ACCEPTANCE PERIOD: Any proposal in response to this solicitation shall be valid for sixty (60) days. At the end of the sixty (60) days, the proposal may be withdrawn at the written request of the Offeror. If the proposal is not withdrawn at that time it remains in effect until an award is made or the solicitation is cancelled.
- E. PROPOSAL PRICES: Proposal prices shall be in the form of a firm unit price for each item during the contract period.
- F. CANCELLATION OF CONTRACT: The purchasing agency reserves the right to cancel and terminate any resulting contract, in part or in whole, without penalty, upon sixty (60) days written notice to the Contractor. In the event the initial contract period is for more than twelve (12) months, the resulting contract may be terminated by either party, without penalty, after the initial twelve (12) months of the contract period upon 60 days written notice to the other party. Any contract cancellation notice shall not relieve the Contractor of the obligation to deliver and/or perform on all outstanding orders issued prior to the effective date of cancellation.
- G. SPECIAL EDUCATIONAL OR PROMOTIONAL DISCOUNTS: The Contractor shall extend any special educational or promotional sale prices or discounts immediately to the Commonwealth during the term of the contract. Such notice shall also advise the duration of the specific sale or discount price.

- H. DRUG FREE WORKPLACE: The Contractor acknowledges and certifies that it understands that the following acts by the Contractor, its employees and/or agents performing services on state property are prohibited:
  1. The unlawful manufacture, distribution, dispensing, possession or use of alcohol or other drugs; and
  2. Any impairment or incapacitation from the use of alcohol or other drugs (except the use of drugs for legitimate medical purposes).
  3. The Contractor further acknowledges and certifies that it understands that a violation of these prohibitions constitutes a breach of contract and may result in default action being taken by the Commonwealth in addition to any criminal penalties that may result from such conduct.
- I. EXTRA CHARGES NOT ALLOWED: The proposal price shall be for complete installation ready for Commonwealth's use, and shall include all applicable freight and installation charges; extra charges will not be allowed.
- J. FINAL INSPECTION: At the conclusion of the work, the Contractor shall demonstrate to the authorized owners representative that the work is fully operational and in compliance with contract specifications and codes. Any deficiencies shall be promptly and permanently corrected by the Contractor at the Contractor's sole expense prior to final acceptance of the work.
- K. IDENTIFICATION OF PROPOSAL: The proposal package should be identified as follows:

From: \_\_\_\_\_

Name of Offeror	Due Date	Time
Street or Box Number	RFP No.	
City, State, Zip Code +4	RFP Title	

Name of Contract / Purchase Officer or Buyer: Jackie Colbert

The package should be addressed as directed on Page 2 of the solicitation.

If a proposal is not clearly identified, the Offeror takes the risk that the proposal may be inadvertently opened and the information compromised which may cause the proposal to be disqualified. Proposals may be hand delivered to the designated location in the office issuing the solicitation. No other correspondence or other proposals should be placed in the envelope.

LATE PROPOSALS: To be considered for selection, proposals must be received by the issuing office by the designated date and hour. The official time used in the receipt of proposals is that time on the automatic time stamp machine in the issuing office. Proposals received in the issuing office after the date and hour designated are automatically disqualified and will not be considered. The University is not responsible for delays in the delivery of mail by the U.S. Postal Service, private couriers, or the intrauniversity mail system. It is the sole responsibility of the Offeror to insure that its proposal reaches the issuing office by the designated date and hour.

- L. INDEMNIFICATION: Contractor agrees to indemnify, defend and hold harmless the Commonwealth of Virginia, its officers, agents, and employees from any claims, damages and actions of any kind or nature, whether at law or in equity, arising from or caused by the use of any materials, goods, or equipment of any kind or nature furnished by the Contractor/any services of any kind or nature furnished by the Contractor, provided that such liability is not attributable to the sole negligence of the using agency or to failure of the using agency to use the materials, goods, or equipment in the manner already and permanently described by the Contractor on the materials, goods, or equipment delivered.



- M. LIMITATION OF LIABILITY: To the maximum extent permitted by applicable law, the Contractor will not be liable under this contract for any indirect, incidental, special or consequential damages, or damages from loss profits, revenue, data or use of the supplies, equipment and/or services delivered under this contract. This limitation of liability will not apply, however, to liability arising from: (a) personal injury or death; (b) defect or deficiency caused by willful misconduct or negligence on the part of the Contractor; or (c) circumstances where the contract expressly provides a right to damages, indemnification or reimbursement.
- N. PRIME CONTRACTOR RESPONSIBILITIES: The Contractor shall be responsible for completely supervising and directing the work under this contract and all subcontractors that he may utilize, using his best skill and attention. Subcontractors who perform work under this contract shall be responsible to the prime Contractor. The Contractor agrees that he is as fully responsible for the acts and omissions of his subcontractors and of persons employed by them as he is for the acts and omissions of his own employees.
- O. RENEWAL OF CONTRACT: This contract may be renewed by the Commonwealth for four (4) successive one (1) year periods under the terms and conditions of the original contract except as stated in 1. below. Price increases may be negotiated only at the time of renewal. Written notice of the Commonwealth's intention to renew should be provided approximately 60 days prior to the expiration date of each contract period:
1. If the Commonwealth elects to exercise the option to renew the contract for an additional one (1) - year period, the contract price(s) for the additional one (1) year shall not exceed the contract price(s) of the previous contract period increased/decreased by more than the percentage increase/decrease of the All Items category of the CPI-W section of the Consumer Price Index of the United States Bureau of Labor Statistics for the latest twelve months for which statistics are available.
- P. SUBCONTRACTS: No portion of the work shall be subcontracted without prior written consent of the purchasing agency. In the event that the Contractor desires to subcontract some part of the work specified herein, the Contractor shall furnish the purchasing agency the names, qualifications and experience of their proposed subcontractors. The Contractor shall, however, remain fully liable and responsible for the work to be done by its subcontractor(s) and shall assure compliance with all requirements of the contract.
- Q. WARRANTY (COMMERCIAL): The Contractor agrees that the supplies or services furnished under any award resulting from this solicitation shall be covered by the most favorable commercial warranties the Contractor gives any customer for such supplies or services and that the rights and remedies provided therein are in addition to and do not limit those available to the Commonwealth by any other clause of this solicitation. A copy of this warranty should be furnished with the proposal.
- R. POLICY OF EQUAL EMPLOYMENT: Virginia Commonwealth University is an equal opportunity/affirmative action employer. Women, Minorities, persons with disabilities are encouraged to apply. The University encourages all vendors to establish and maintain a policy to insure equal opportunity employment. To that end, Offerors should submit along with their proposals, their policy of equal employment.
- S. eVA BUSINESS-TO-GOVERNMENT CONTRACTS AND ORDERS: The solicitation/contract will result in purchase order(s) with the eVA transaction fee specified below assessed for each order.
1. For orders issued July 1, 2011 thru June 30, 2013, the Vendor Transaction Fee is:
    - a) DSBSD-certified Small Businesses: 0.75%, Capped at \$500 per order.
    - b) Businesses that are not DSBSD-certified Small Businesses: 0.75%, Capped at \$1,500 per order.
  2. For orders issued July 1, 2013, and after, the Vendor Transaction Fee is:
    - a) DSBSD-certified Small Businesses: 1%, Capped at \$500 per order.

- b) Businesses that are not DSBSD-certified Small Businesses: 1%, Capped at \$1,500 per order.

The specified vendor transaction fee will be invoiced, by the Commonwealth of Virginia Department of General Services, approximately 30 days after the corresponding purchase order is issued and payable 30 days after the invoice date. Any adjustments (increases/decreases) will be handled through purchase order changes.

The eVA Internet electronic procurement solution, website portal [www.eva.virginia.gov](http://www.eva.virginia.gov), streamlines and automates government purchasing activities in the Commonwealth. The portal is the gateway for vendors to conduct business with state agencies and public bodies.

Vendors desiring to provide goods and/or services to the Commonwealth shall participate in the eVA Internet e-procurement solution and agree to comply with the following: If this solicitation is for a term contract, may provide an electronic catalog (price list) or index page catalog for items awarded. The format of this electronic catalog shall conform to the eVA Catalog Interchange Format (CIF) Specification that can be accessed and downloaded from [www.eVA.virginia.gov](http://www.eVA.virginia.gov). Contractors should email Catalog or Index Page information to [eVA-catalog-manager@dgs.virginia.gov](mailto:eVA-catalog-manager@dgs.virginia.gov).

- T. GRAMM-LEACH-BLILEY ACT: The Contractor shall comply with the Act by implementing and maintaining appropriate safeguards to protect and prevent unauthorized release of student, faculty and staff nonpublic information. Nonpublic information is defined as social security numbers, or financial transactions, bank, credit and tax information.
- U. DETERMINATION OF RESPONSIBILITY: The Contract will be awarded to the responsive and responsible Offeror with a Proposal, conforming to the RFP, will be most advantageous to VCU, technical and financial factors considered. A responsible Offeror is one who affirmatively demonstrates to VCU that it has adequate financial resources and the requisite capacity, capability, and facilities to perform the Contract, has a satisfactory record of performance on other comparable projects, has a satisfactory record of integrity and business ethics, and is otherwise qualified and eligible to receive award under the solicitation and laws and regulations applicable to the procurement. VCU reserves the right to investigate the capabilities of Offeror, confirm any part of the information furnished by an Offeror, and require other evidence to determine that the Offeror is responsible.
- V. REJECTION OF PROPOSALS & WAIVER OF MINOR INFORMALITIES/IRREGULARITIES: VCU reserves the right to reject any or all Proposals in part or in total for any reason, to accept any Proposal if considered best for its interest, and to waive informalities and minor irregularities in Proposals received, commensurate with best public procurement practices.
- W. PROTEST: Any Offeror who desires to protest the award or decision to award a Contract shall submit the protest in writing to:

Director of Procurement Services  
Virginia Commonwealth University  
912 West Grace, 5<sup>th</sup> Floor  
Richmond, VA 23284

VCU will announce the award utilizing the Commonwealth of Virginia's e-Procurement system (eVA). The protest must be received no later than ten (10) days after the award or the announcement of the decision to award, whichever occurs first. However, if the protest of any actual or potential Offeror depends in whole or in part upon information contained in public records pertaining to the procurement transaction that are subject to inspection under the Rules Governing Procurement of Goods, Services, Insurance, and Construction by a Public Institution of Higher Education of the Commonwealth of Virginia Governed by Subchapter 3 of the Restricted Higher Education Financial and Administrative Operations Act,, Chapter 4.10 (§23-38.88 et seq) of Title 23 of the Code of Virginia, §34, then the time within which the protest shall be submitted

shall expire ten (10) days after those records are available for inspection by such Offeror under §34, or at such later time as provided in this section.

VCU Notices of Award(s) or Notices of Intent to Award may be accessed electronically at <http://www.eva.virginia.gov>.

No protest shall lie for a claim that the selected Offeror is not a responsible Offeror.

The written protest shall include the basis for the protest and relief sought.

The VCU Director of Procurement Services shall issue a decision in writing within ten (10) days of receipt stating the reasons for the action taken. This decision shall be final unless the Offeror appeals within ten (10) days of receipt of the written decision by instituting legal action as provided in Section 54 of the Governing Rules.

Nothing in this paragraph shall be construed to permit a proposer to challenge the validity of the terms or conditions of the RFP.

"Days" as used in this paragraph refer to calendar days. If a deadline falls on a Saturday or Sunday, the next business day shall be considered to be the deadline.

## **XII. SPECIAL TERMS AND CONDITIONS INFORMATION TECHNOLOGY:**

- A. **QUALIFIED REPAIR PERSONNEL:** All warranty or maintenance services to be performed on the items specified in this solicitation as well as any associated hardware or software shall be performed by qualified technicians properly authorized by the manufacturer to perform such services. The Commonwealth reserves the right to require proof of certification prior to award and at any time during the term of the contract.
- B. **SOURCE CODE:** In the event the contractor ceases to maintain experienced staff and the resources needed to provide required software maintenance, the Commonwealth shall be entitled to have use, and duplicate for its own use, a copy of the source code and associated documentation for the software products covered by the contract. Until such time as a complete copy of such material is provided, the Commonwealth shall have exclusive right to possess all physical embodiments of such contractor owned materials. The rights of the Commonwealth in this respect shall survive for a period of twenty years after the expiration or termination of the contract. All lease and royalty fees necessary to support this right are included in the initial license fee as contained in the pricing schedule.
- C. **SOFTWARE UPGRADES:** The Commonwealth shall be entitled to any and all upgraded versions of the software covered in the contract that becomes available from the contractor. The maximum charge for upgrade shall not exceed the total difference between the cost of the Commonwealth's current version and the price the contractor sells or licenses the upgraded software under similar circumstances.
- D. **THIRD PARTY ACQUISITION OF SOFTWARE:** The contractor shall notify the procuring agency in writing should the intellectual property, associated business, or all of its assets be acquired by a third party. The contractor further agrees that the contract's terms and conditions, including any and all license rights and related services, shall not be affected by the acquisition. Prior to completion of the acquisition, the contractor shall obtain, for the Commonwealth's benefit and deliver thereto, the assignee's agreement to fully honor the terms of the contract.
- E. **TITLE OF SOFTWARE:** By submitting a proposal, the offeror represents and warrants that it is the sole owner of the software or, if not the owner, that it has received all legally required authorizations from the owner to license the software, has the full power to grant the rights required by this solicitation, and that neither the software nor its use in accordance with the

contract will violate or infringe upon any patent, copyright, trade secret, or any other property rights of another person or organization.

- F. WARRANTY AGAINST SHUTDOWN DEVICES: The contractor warrants that the equipment and software provided under the contract shall not contain any lock, counter, CPU references, virus, worm, or other device capable of halting operations or erasing or altering data or programs. Contractor further warrants that neither it, nor its agents, employees, or subcontractors shall insert any shutdown device following delivery of the equipment and software.
- G. SECTION 508 COMPLIANCE: All information technology which, pursuant to this Contract, is purchased or upgraded by or for the use of any Commonwealth agency or institution or political subdivision of the Commonwealth (the "Technology") shall comply with Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended. If requested, the Contractor must provide a detailed explanation of how compliance with Section 508 of the Rehabilitation Act is achieved and a validation of concept demonstration. The requirements of this Paragraph along with the Non-Visual Access to Technology Clause shall be construed to achieve full compliance with the Information Technology Access Act, §§ 2.2-3500 through 2.2-3504 of the *Code of Virginia*.
- H. NONVISUAL ACCESS TO TECHNOLOGY: All information technology which, pursuant to this Agreement, is purchased or upgraded by or for the use of any State agency or institution or political subdivision of the Commonwealth (the "Technology") shall comply with the following nonvisual access standards from the date of purchase or upgrade until the expiration of this Agreement:
1. effective, interactive control and use of the Technology shall be readily achievable by nonvisual means;
  2. the Technology equipped for nonvisual access shall be compatible with information technology used by other individuals with whom any blind or visually impaired user of the Technology interacts;
  3. nonvisual access technology shall be integrated into any networks used to share communications among employees, program participants or the public; and
  4. the technology for nonvisual access shall have the capability of providing equivalent access by nonvisual means to telecommunications or other interconnected network services used by persons who are not blind or visually impaired.

Compliance with the foregoing nonvisual access standards shall not be required if the head of the using agency, institution or political subdivision determines that (i) the Technology is not available with nonvisual access because the essential elements of the Technology are visual and (ii) nonvisual equivalence is not available.

Installation of hardware, software, or peripheral devices used for nonvisual access is not required when the Technology is being used exclusively by individuals who are not blind or visually impaired, but applications programs and underlying operating systems (including the format of the data) used for the manipulation and presentation of information shall permit the installation and effective use of nonvisual access software and peripheral devices.

If requested, the Contractor must provide a detailed explanation of how compliance with the foregoing nonvisual access standards is achieved and a validation of concept demonstration.

The requirements of this Paragraph shall be construed to achieve full compliance with the Information Technology Access Act, §§ 2.1-807 through 2.1-811 of the *Code of Virginia*.

I. DATA AND INTELLECTUAL PROPERTY PROTECTION:

1. Definitions
  - a. "End User" means the individuals authorized by the University to access and use the Services provided by the Selected Firm/Vendor under this agreement.
  - b. "Personally Identifiable Information" includes but is not limited to: personal identifiers such as name, address, phone number, date of birth, Social Security number, and student or

personnel identification number; “personal information” as defined in Virginia Code section 18.2-186.6 and/or any successor laws of the Commonwealth of Virginia; personally identifiable information contained in student education records as that term is defined in the Family Educational Rights and Privacy Act, 20 USC 1232g; “medical information” as defined in Virginia Code Section 32.1-127.1:05; “protected health information” as that term is defined in the Health Insurance Portability and Accountability Act, 45 CFR Part 160.103; nonpublic personal information as that term is defined in the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 USC 6809; credit and debit card numbers and/or access codes and other cardholder data and sensitive authentication data as those terms are defined in the Payment Card Industry Data Security Standards; other financial account numbers, access codes, driver’s license numbers; and state- or federal-identification numbers such as passport, visa or state identity card numbers.

- c. “Securely Destroy” means taking actions that render data written on physical (e.g., hardcopy, microfiche, etc.) or electronic media unrecoverable by both ordinary and extraordinary means. These actions must meet or exceed those sections of the National Institute of Standards and Technology (NIST) SP 800-88 guidelines relevant to data categorized as high security.
- d. “Security Breach” means a security-relevant event in which the security of a system or procedure used to create, obtain, transmit, maintain, use, process, store or dispose of data is breached, and in which University Data is exposed to unauthorized disclosure, access, alteration, or use.
- e. “Services” means any goods or services acquired by the University of Virginia from the Selected Firm/Vendor.
- f. “University Data” includes all Personally Identifiable Information and other information that is not intentionally made generally available by the University on public websites or publications, including but not limited to business, administrative and financial data, intellectual property, and patient, student and personnel data.

## 2. Rights and License in and to the University Data

The parties agree that as between them, all rights including all intellectual property rights in and to University Data shall remain the exclusive property of the University, and Selected Firm/Vendor has a limited, nonexclusive license to use these data as provided in this agreement solely for the purpose of performing its obligations hereunder. This agreement does not give a party any rights, implied or otherwise, to the other’s data, content, or intellectual property, except as expressly stated in the agreement.

## 3. Intellectual Property Disclosure/Rights

- a. Unless expressly agreed to the contrary in writing, all goods, products, materials, documents, reports, writings, video images, photographs or papers of any nature including software or computer images prepared by Selected Firm/Vendor (or its subcontractors) for the University will not be disclosed to any other person or entity without the written permission of the University.
- b. Selected Firm/Vendor warrants to the University that the University will own all rights, title and interest in any intellectual property created for the University as part of the performance of this agreement and will have full ownership and beneficial use thereof, free and clear of claims of any nature by any third party including, without limitation, copyright or patent infringement claims. Selected Firm/Vendor agrees to assign and hereby assigns all rights, title, and interest in any and all intellectual property created for the University as part of the performance of this agreement to the University, and will execute any future assignments or other documents needed for the University to document, register, or otherwise perfect such rights. Nothing in this section is, however, intended to or shall be construed to apply to existing intellectual property created or owned by the vendor that the University is licensing under this agreement. For avoidance

of doubt, the University asserts no intellectual property ownership under this clause to any pre-existing intellectual property of the vendor, and seeks ownership rights only to the extent Vendor is being engaged to develop certain intellectual property as part of its services for the University.

- c. Notwithstanding the foregoing, for research collaboration pursuant to subcontracts under sponsored research agreements administered by the University's Office of Sponsored Programs, intellectual property rights will be governed by the terms of the grant or contract to the University to the extent such grant or contract requires intellectual property terms to apply to subcontractors.

#### 4. Data Privacy

- a. Selected Firm/Vendor will use University Data only for the purpose of fulfilling its duties under this agreement and will not share such data with or disclose it to any third party without the prior written consent of the University, except as required by this agreement or as otherwise required by law.
- b. University Data will not be stored outside the United States without prior written consent from the University.
- c. Selected Firm/Vendor will provide access to University Data only to its employees and subcontractors who need to access the data to fulfill Selected Firm/Vendor obligations under this agreement. Selected Firm/Vendor will ensure that employees who perform work under this agreement have read, understood, and received appropriate instruction as to how to comply with the data protection provisions of this agreement.
- d. The following provision applies only if Selected Firm/Vendor will have access to the University's education records as defined under the Family Educational Rights and Privacy Act (FERPA): The Selected Firm/Vendor acknowledges that for the purposes of this agreement it will be designated as a "school official" with "legitimate educational interests" in the University education records, as those terms have been defined under FERPA and its implementing regulations, and the Selected Firm/Vendor agrees to abide by the limitations and requirements imposed on school officials. Selected Firm/Vendor will use the education records only for the purpose of fulfilling its duties under this agreement for University's and its End User's benefit, and will not share such data with or disclose it to any third party except as provided for in this agreement, required by law, or authorized in writing by the University.

#### 5. Data Security

- a. Selected Firm/Vendor will store and process University Data in accordance with commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure Selected Firm/Vendor's own data of a similar type, and in no event less than reasonable in view of the type and nature of the data involved. Without limiting the foregoing, Selected Firm/Vendor warrants that all electronic University Data will be encrypted in transmission (including via web interface) in accordance with latest version of National Institute of Standards and Technology Special Publication 800-53.
- b. If the Selected Firm/Vendor stores Personally Identifiable Information as part of this agreement, the Selected Firm/Vendor warrants that the information will be stored in accordance with latest version of National Institute of Standards and Technology Special Publication 800-53.
- c. Selected Firm/Vendor will use industry-standard and up-to-date security tools and technologies such as anti-virus protections and intrusion detection methods in providing Services under this agreement.

#### 6. Employee Background Checks and Qualifications

Selected Firm/Vendor shall ensure that its employees who will have potential access to University Data have passed appropriate, industry standard, background screening and possess the qualifications and training to comply with the terms of this agreement.

7. Data Authenticity and Integrity

Selected Firm/Vendor will take reasonable measures, including audit trails, to protect University Data against deterioration or degradation of data quality and authenticity. The Selected Firm will be responsible during the terms of this agreement, unless otherwise specified elsewhere in this agreement, for converting and migrating electronic data as often as necessary so that information is not lost due to hardware, software, or media obsolescence or deterioration.

8. Security Breach

a. Response. Upon becoming aware of a Security Breach, or of circumstances that are reasonably understood to suggest a likely Security Breach, Selected Firm/Vendor will timely notify the University consistent with applicable state or federal laws, fully investigate the incident, and cooperate fully with the University's investigation of and response to the incident. Except as otherwise required by law, Selected Firm/Vendor will not provide notice of the incident directly to individuals whose Personally Identifiable Information was involved, regulatory agencies, or other entities, without prior written permission from the University.

b. Liability.

- 1) If Selected Firm/Vendor must under this agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of University Data known as Personally Identifiable Information, the following provisions apply. In addition to any other remedies available to the University under law or equity, Selected Firm/Vendor will reimburse the University in full for all costs incurred by the University in investigation and remediation of any Security Breach caused by Selected Firm/vendor, including but not limited to providing notification to individuals whose Personally Identifiable Information was compromised and to regulatory agencies or other entities as required by law or contract; providing one year's credit monitoring to the affected individuals if the Personally Identifiable Information exposed during the breach could be used to commit financial identity theft; and the payment of legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Security Breach.
- 2) If Selected Firm/Vendor will NOT under this agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of University Data known as Personally Identifiable Information, the following provisions apply. In addition to any other remedies available to the University under law or equity, Selected Firm/Vendor will reimburse the University in full for all costs reasonably incurred by the University in investigation and remediation of any Security Breach caused by Selected Firm/vendor.

9. Response to Legal Orders, Demands or Requests for Data

a. Except as otherwise expressly prohibited by law, Selected Firm/Vendor will:

- immediately notify the University of any subpoenas, warrants, or other legal orders, demands or requests received by Selected Firm/Vendor seeking University Data;
- consult with the University regarding its response;
- cooperate with the University's reasonable requests in connection with efforts by the University to intervene and quash or modify the legal order, demand or request; and
- upon the University's request, provide the University with a copy of its response.

- b. If the University receives a subpoena, warrant, or other legal order, demand (including request pursuant to the Virginia Freedom of Information Act) or request seeking University Data maintained by Selected Firm/Vendor, the University will promptly provide a copy to Selected Firm/Vendor. Selected Firm/Vendor will promptly supply the University with copies of data required for the University to respond, and will cooperate with the University's reasonable requests in connection with its response.
10. Data Transfer Upon Termination or Expiration
  - a. Upon termination or expiration of this agreement, Selected Firm/Vendor will ensure that all University Data are securely returned or destroyed as directed by the University in its sole discretion. Transfer to the University or a third party designated by the University shall occur within a reasonable period of time, and without significant interruption in service. Selected Firm/Vendor shall ensure that such transfer/migration uses facilities and methods that are compatible with the relevant systems of the University or its transferee, and to the extent technologically feasible, that the University will have reasonable access to University Data during the transition. In the event that the University requests destruction of its data, Selected Firm/Vendor agrees to Securely Destroy all data in its possession and in the possession of any subcontractors or agents to which the Selected Firm/Vendor might have transferred University data. The Selected Firm/Vendor agrees to provide documentation of data destruction to the University.
  - b. Selected Firm/Vendor will notify the University of impending cessation of its business and any contingency plans. This includes immediate transfer of any previously escrowed assets and data and providing the University access to Selected Firm/Vendor's facilities to remove and destroy University-owned assets and data. Selected Firm/Vendor shall implement its exit plan and take all necessary actions to ensure a smooth transition of service with minimal disruption to the University. Selected Firm/Vendor will also provide a full inventory and configuration of servers, routers, other hardware, and software involved in service delivery along with supporting documentation, indicating which if any of these are owned by or dedicated to the University. Selected Firm/Vendor will work closely with its successor to ensure a successful transition to the new equipment, with minimal downtime and effect on the University, all such work to be coordinated and performed in advance of the formal, final transition date.
11. Audits
  - a. The University reserves the right in its sole discretion to perform audits of Selected Firm/Vendor at the University's expense to ensure compliance with the terms of this agreement. The Selected Firm/Vendor shall reasonably cooperate in the performance of such audits. This provision applies to all agreements under which the Selected Firm/Vendor must create, obtain, transmit, use, maintain, process, or dispose of University Data.
  - b. If the Selected Firm/Vendor must under this agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of University Data known as Personally Identifiable Information or financial or business data which has been identified to the Selected Firm/Vendor as having the potential to affect the accuracy of the University's financial statements, Selected Firm/Vendor will at its expense conduct or have conducted at least annually a:
    - American Institute of CPAs Service Organization Controls (SOC 2) Type II audit, or other security audit with audit objectives deemed sufficient by the University, which attests the Selected Firm/Vendor's security policies, procedures and controls;
    - vulnerability scan of Selected Firm/Vendor's electronic systems and facilities that are used in any way to deliver electronic services under this agreement; and
    - formal penetration test of Selected Firm/Vendor's electronic systems and facilities that are used in any way to deliver electronic services under this agreement.



Additionally, the Selected Firm/Vendor will provide the University upon request the results of the above audits, scans and tests, and will promptly modify its security measures as needed based on those results in order to meet its obligations under this agreement. The University may require, at University expense, the Selected Firm/Vendor to perform additional audits and tests, the results of which will be provided promptly to the University.

12. Compliance

- a. Selected Firm/Vendor will comply with all applicable laws and industry standards in performing services under this agreement. Any Selected Firm/Vendor personnel visiting the University's facilities will comply with all applicable University policies regarding access to, use of, and conduct within such facilities. The University will provide copies of such policies to Selected Firm/Vendor upon request.
- b. Selected Firm/Vendor warrants that the service it will provide to the University is fully compliant with relevant laws, regulations, and guidance that may be applicable to the service, such as: the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH), Gramm-Leach-Bliley Financial Modernization Act (GLB), Payment Card Industry Data Security Standards (PCI-DSS), Americans with Disabilities Act (ADA), Federal Export Administration Regulations, and Defense Federal Acquisitions Regulations.
- c. If the Payment Card Industry Data Security Standards (PCI-DSS) are applicable to the Selected Firm/Vendor service provided to the University, the Selected Firm/Vendor will, upon written request, furnish proof of compliance with PCI-DSS within 10 business days of the request.

13. No End User agreements

This agreement is the entire agreement between the University (including University employees and other End Users) and the Selected Firm/Vendor. In the event that the Selected Firm/Vendor enters into terms of use agreements or other agreements or understandings, whether electronic, click-through, verbal or in writing, with University employees or other End Users, such agreements shall be null, void and without effect, and the terms of this agreement shall apply.

14. Survival

The Selected Firm/Vendor's obligations under Section 10 shall survive termination of this agreement until all University Data has been returned or securely destroyed.

**XIII. CONTRACT ADMINISTRATION:**

Upon award of the contract VCU shall designate, in writing, the name(s) of the Contract Administrator(s) who shall work with the contractor in formulating mutually acceptable plans and standards for the delivery, installation and on-going service and/or maintenance that may be required.

- A. The Contract Administrator shall use all powers under the contract to enforce its faithful performance. The Contract Administrator shall determine the amount, quality and acceptability of work and shall decide all other questions in connection with the work.
- B. All direction and orders from VCU shall be transmitted through the Contract Administrator, or his designee. However the Contract Administrator shall have no authority to order changes in the work which alter the concept or scope of the work or change the basis for compensation to the contractor.

**XIV. ATTACHMENTS:**

A: Schedule A

B: Appendix I – Participation In State Procurement Transactions Small Businesses and Businesses Owned By Women and Minorities:

[http://procurement.vcu.edu/media/procurement/pdf/document-library/RFP\\_Website\\_Link\\_Appendix\\_1.pdf](http://procurement.vcu.edu/media/procurement/pdf/document-library/RFP_Website_Link_Appendix_1.pdf)

C: Appendix II – Invoicing and Payment

[http://procurement.vcu.edu/media/procurement/pdf/document-library/RFP\\_Website\\_Link\\_Appendix\\_2.pdf](http://procurement.vcu.edu/media/procurement/pdf/document-library/RFP_Website_Link_Appendix_2.pdf)



RFP - Addendum

---

DATE: October 26, 2016

ADDENDUM NO. 01 TO ALL OFFERORS:

Reference - Request for Proposals: RFP# 7216216JC

Commodity/Title:	Identity and Access Management (IAM) Software and Services
Issue Date:	October 17, 2016
Proposal Due:	November 17, 2016 at 11:00 AM

The above is hereby changed to read: **See Attached.**

NOTE: A signed acknowledgment of this addendum must be received by this office either prior to the proposal due date and hour or attached to your proposal. Signature of this addendum does not constitute your signature on the original proposal document. The original proposal document must also be signed.

Very truly yours,

Jackie Colbert

---

Name of Firm

---

Signature/Title

---

Date

Reference Page 5, Section IV., PRE-PROPOSAL CONFERENCE:

Offerors may participate in the optional pre-proposal conference via conference call by:

- Using the following “Dial-In” numbers:
- 866-842-5779 (United States & Canada);
- 832-445-3763 (International);
- Using Conference Code #: 8415263709
- Dialing the appropriate “Dial-In” number at the scheduled time; and
- Entering the “Conference Code” when prompted, followed by the “#.”

Note: Offerors who participated in the pre-proposal conference via conference call shall submit an email to [jcolbert@vcu.edu](mailto:jcolbert@vcu.edu) within one (1) business day of the pre-proposal conference, confirming the Offerors participation and the Offeror’s contact information.



RFP - Addendum

---

DATE: November 2, 2016

ADDENDUM NO. 02 TO ALL OFFERORS:

Reference - Request for Proposals: RFP #7216216JC

Commodity/Title: Identity and Access Management (IAM) Software  
and Services

Issue Date: October 17, 2016

Proposal Due: November 17, 2016 at 11:00 AM

Pre-Proposal Conference: October 31, 2016 at 2:00 PM

The above is hereby changed to read: **See Attached.**

NOTE: A signed acknowledgment of this addendum must be received by this office either prior to the proposal due date and hour or attached to your proposal. Signature of this addendum does not constitute your signature on the original proposal document. The original proposal document must also be signed.

Very truly yours,

Jackie Colbert  
Procurement Services  
Information Technology Category Manager and Contracting Officer

---

Name of Firm

---

Signature/Title

---

Date

Questions for Clarification Submitted By Potential Offerors for RFP# 7216216JC

The questions submitted by potential proposers and the answers from VCU are below. The clarifications are in blue.

1. Regarding Attachment A, Security Data - If an Offeror is proposing an IDaaS solution, how does VCU anticipate IDaaS providers respond to on-premise questions included in Attachment A?

For IDaaS solution providers, the Offeror is expected to provide requested security and management documentation as requested in the cloud section. These documents are expected to effectively address the questions from the on-premises section, in addition to other applicable administrative, technical and physical controls related to its infrastructure, applications, personnel and processes. For on-premises questions, the Offeror should provide excerpts from the aforementioned documents and / or provide references back to these documents.

2. T-ARCH-062 Architecture Requirements - What type of mobile devices are you concerned with? Android, iPhone, etc.? We are BYOD environment. We would like to have support for Android, iOS or any other mainstream devices.

Ref.	Category	RFP Question	Clarification Question	VCU Response
T-ARCH-062	Architecture Requirements	Is the application optimized for mobile device support including a responsive user interface or app? What is supported out of the box?	What type of mobile devices are you concerned with? Android, iPhone, etc.?	Please describe what mobile capabilities your solution supports out-of-the-box with regards to user interfaces. As VCU is a "BYOD" organization, please outline what support you solution has for Android, iOS or any other mainstream mobile operating systems and respective mobile browsers.

3. T-CR-004 Compliance Requirements - What type of events are you concerned about? Who provisioned what?

Ability to track the creation, access, modification, and deletion of records, including but not limited to administrative actions such as the change of roles and access, check-in / check-out of privileged accounts and addition, modification or removal of

identities and groups. At a minimum, these events should provide the action that was performed, the identity that performed the action, and adequate timestamp of the action.

4. T-IAI-256 Identity and Access Intelligence- What type of customizations do you anticipate?

Ref.	Category	RFP Question	Clarification Question	VCU Response
T-IAI-256	Identity and Access Intelligence	Can pre-defined reports be personalized by end users to fit their specific business needs?	What type of customizations do you anticipate?	Please describe what is possible with your solution, such as ability to add and remove columns, ability to customize query, etc.

5. T-RM-152 Role Management - Do you mean via who your manager is listed in AD or from some sort of file (CSV, etc.) Could you elaborate?

Ref.	Category	RFP Question	Clarification Question	VCU Response
T-RM-152	Role Management	Does the solution support the ability to read or import organizational hierarchy information?	Do you mean via who your manager is listed in AD or from some sort of file (CSV, etc.) Could you elaborate?	Please describe what capabilities your solution is able to support. Yes, manager information in a CSV is one way to do read org information, but may not necessarily be the only way.

6. T-SR-009 Security Requirements - Could you elaborate further? Not sure what you mean on SSO integration points/options.

Ref.	Category	RFP Question	Clarification Question	VCU Response
T-SR-009	Security Requirements	Please describe this system's Role Based	Could you elaborate further? Not	We are interested to learn about the solution's ability to push

		Access Control capabilities, please include any Directory or SSO integration points and options.	sure what you mean on SSO integration points/options.	and pull objects and access permissions to and from directories with which it integrate. Further, we are interested to learn about its ability to provide digestible object, role, and permission information to Single Sign-On platforms (SSO), so these platforms can be used for both authentication and authorization to various systems and applications. We will need to know with what directory and SSO platforms can the system integrate, and what information can be transmitted and digested to and from these platforms.
--	--	--	---	---

7. PS-INTEG-016 Enterprise Integrations - What is the enterprise mail system? Exchange, Google, O365?

We are primarily a Google mail environment. We have two name spaces, one for students and one for employees, faculty and staff. We also have Office 365 for some of our user base.

8. PS-LCM-021 Identity Lifecycle Requirements - Is there an attribute in AD or something else to determine the type of user? If so what is it?

Ref.	Category	RFP Question	Clarification Question	VCU Response
PS-LCM-021	Identity Lifecycle Requirements	Must be able to identify primary types of users (students, faculty, staff, affiliates, etc.) and provision	Is there an attribute in AD or something else to determine the type of	We have several high level attributes that define users affiliation or role. We use a variation of eduPerson schema in our



		access based this information. These primary types (i.e. enterprise roles, business roles, etc.) of users are not mutually exclusive, as a user can be a staff member and student at the same time.	user? If so what is it?	enterprise directories. There about 10 major affiliations, i.e. faculty, employee, student, member.
--	--	---	-------------------------	---

9. T-SD-009 Security of Data (On-Premise) - Is this in reference to their AD account?

This is in reference to accounts authorized to access the system. Examples include the administrator of the IAM system logging in to the application for maintenance purposes, or an HR director logging into the system to view the dashboard.

10. The Identity and Access Management RFP includes a complex set of specifications, including a number of integrations that will require Offeror analysis and scope development. The RFP also includes a large number of technical, functional, and implementation questions that Offerors are required to address. We respectfully request an extension of the response due date until December 8 (taking into account the short Thanksgiving week) to allow Offerors adequate time to develop responsive proposals.

We will not be extending the response due date.

11. Reference: V. – Statement of needs, Pages 5-6

Question: We would appreciate VCU's input on the following questions about your current environment and the scope of the IAM project:

- a. Does VCU expect the solution to be a leverage as a SaaS (software as a service) or deployed on-premise?

VCU is open to both approaches and will evaluate either approach based on functionality and risk.

- b. How many environments does VCU wants the solution implemented in (for example, DEV, UAT, PROD)?

UAT and PROD.

- c. Is Disaster Recovery in scope for the initial delivery stage, or is that something that VCU will build at a later time?

Yes, two sites will be required with one serving as a disaster-recovery site.

- d. Are there any virtualization platforms available in the VCU environment (for example, VMware ESX)? If yes, what version(s)?

VCU utilizes VMware vSphere infrastructure. The hypervisors are currently operating on VMware ESXi 6.0.

- e. Is there a number of VCU staff and individuals already identified to work with the deployed solution to administer it and configure it during the delivery project and after the solution delivery is completed?

VCU anticipates dedicated and partially-dedicated staff to assist with the deployment and ongoing administration of the solution. Please clarify what your expectations and assumptions are with regards to VCU-committed resources.

- f. What is the envisioned number of VCU FTEs assigned to this project and solution?

Same as 11 e above.

12. Will VCU accept estimated Time and Material (T&M) pricing for the implementation services for the IAM solution and required integrations?

No.

13. What are VCU's preferred IaaS and/or PaaS platforms, i.e. AWS, Azure, Cloud Foundry, etc...?

VCU currently does not officially have a preferred IaaS or PaaS platform, but is open to solution proposals utilizing reputable IaaS and / or PaaS providers such as Amazon AWS or Microsoft Azure.

14. For "Does this system provide native compatibility for the following database architectures SQL, Oracle or additional database support?" please define "native compatibility, i.e. as an Identity Repository, an AuthN/Z Store, a Provisioning Target, etc...?"

Ref.	Category	RFP Question	Clarification Question	VCU Response
T-ARCH-061	Architecture Requirements	Does this system provide native compatibility for the following database architectures SQL, Oracle or additional database support?	For "Does this system provide native compatibility for the following database architectures SQL, Oracle or additional database support?" please define "native compatibility, i.e. as an Identity Repository, an AuthN/Z Store, a Provisioning Target, etc?	If a database layer is required, please describe which SQL databases you support, and in which ways your databases are deployed. This is not intended to define your SQL provisioning target systems.

15. For "Can the solution support collecting data from SaaS applications (e.g., Google Apps for Education, Office 365, Salesforce.com, etc.)?" What information needs to be collected from these and other SaaS apps/for what purpose?

Ref.	Category	RFP Question	Clarification Question	VCU Response
T-DAC-297	Data Aggregation and Correlation	Can the solution support collecting data from SaaS applications (e.g., Google Apps for Education, Office 365, Salesforce.com, etc.)?	For "Can the solution support collecting data from SaaS applications (e.g., Google Apps for Education, Office 365, Salesforce.com, etc.)?" What information needs to be collected from these and other SaaS apps/for what purpose?	Please describe what your solution is capable of collecting from SaaS applications such as information and metadata about accounts, entitlements (i.e. groups, roles, permissions), assigned access. This does not include data-access governance (DAG) features.

16. Do you want one single vendor to provide you with Identity Management, Access Management, Single sign on, Federated Identity Management, and Directory server solutions for this RFP?

VCU prefers one vendor. However, we are not specifically seeking a solution to provide single sign-on (federated single sign-on, web-access management, etc.) this time.

17. Is second factor authentication part of this RFP?

We currently use DUO as a second factor. Your solution is not required to replace Duo, but your solution must be able to integrate and use Duo as an additional factor.

18. Do you want captcha to be part of this IAM solution?

No.

19. Under your current Federation solution is VCU only an Identity Provider or also as a Service Provider or both?

Yes, we perform both functions as an identity provider (IdP) and Service Provider (SP). We are part of InCommon. However, with this solution selection we are not looking to evaluate federated single sign-on capabilities that SAML or OAuth provide.

20. Are you looking for a virtual solution or a physical hardware appliance solution?

Virtual preferred.

21. As a Offeror is it possible to propose pricing for the virtual IAM Solution and also for a hardware Appliance Solution?

Yes.

22. Do you have any other Operating Systems at VCU which eventually part of this new environment beside what has been mentioned in the RFP?

Ref.	Category	RFP Question	Clarification Question	VCU Response
n/a	n/a	n/a	Do you have any other Operating Systems at VCU which eventually part of this new environment beside what has been mentioned in the RFP?	The Operating Systems listed on Page 6 are those planned to be supported by VCU, on which your solution will be installed (assuming an on-premise solution). If you anticipate plans for a different operating system please provide details.

23. In the RFP you have currently sixteen (16) applications as part of this RFP – How many actual web and non-web applications will VCU eventually have for this environment?

We have not determined a number. We only determined the centrally managed applications that made sense for the initial implementation. We will add applications as needed.

24. Will Shibboleth be one of the supported application or will be migrated to the new proposed Federation solution?

VCU will continue to maintain CAS.

25. Will VCU continue to maintain CAS 3.5.3 as their Single Sign-on solution? Or will be migrated to the new proposed Federation solution?

VCU will continue to maintain CAS.

26. Do you want to include or consider a migration plan from Shibboleth IDP and CAS to a newly proposed Federated Identity Management and Single sign-on solution?

We will address SSO solutions at a later time.

27. What is the name of the application for your HR Record? Do you want us to design to receive daily feed from your HR System?

Ellucian Banner. We want real time updates and batch updates as it is deemed necessary.

28. Will you still like to maintain Active Directory as your Directory Server solution or for authentication and authorization system?

Yes, we will continue to use Active Directory as one of our authentication and authorization systems. VCU also uses NetIQ eDirectory as a directory solution.

29. Do you want this solution to have self-services capabilities built-in so the users can reset password, send request to elevate their permission to use their application or request access to certain application within VCU?

Yes.

30. How many users within the each applications? Are they are external or internal users or both?

Please refer to Page 6 of Request for Proposal. Clarify external (alumni, vendors. Etc...?) and internal (active accounts). Please visit the following site for statistical information and institutional data about VCU, our students and faculty/staff:  
<http://www.opds.vcu.edu/>

31. Out of 231,352 users how many users are external users? What is your yearly growth?

We add roughly 18,000 accounts a year. On average we have about 80,000 active (enabled) accounts.

32. How your internal and external users are authenticate and get authorization for their respective applications?

We currently use Federation, eDirectory and Active Directory.

33. Where do the users, groups and roles reside? Do you have separate Directory Server or LDAP for your internal and external users?

We currently use attributes and groups to determine some major roles of users. They are contained within several databases and directories, mostly within eDirectory and Active Directory.

34. Do your external users consist of former students, alumni, vendor and contractors? And what is the procedure in place adding, deleting and modifying your users?

We have one directory that contains all users that have been at the university since 2005. Users that are previous to this time are added as needed. Our vendors are inserted into our ERP as affiliates and are issued an id in the same system as all other users.

35. Do you want IAM Solution to implement life cycle rule (for an example: password expiration, recertification process etc.)?

Yes.

36. Do you want this IAM solution to provide you with govern access and ensure regulatory compliance, segregation of duties etc...?

This can be an option, but it is not required at this stage.

37. Are the terms and conditions of the RFP Negotiable? This procurement is for Commercial Off-The Shelf software licenses, and thus requires the Commercial Licensing Agreement be incorporated, particularly for the usage rights and limitations of the software.

The terms and conditions of the RFP govern the contract. VCU will consider additional terms and conditions regarding licensing and intellectual property.

38. Is this a small business set aside? Contractor does not intend to use any small businesses in this response, so that would preclude Contractor from being able to bid on this opportunity.

The IAM RFP is not a small business set aside.

39. It was noticed that Integral Partners was hired to help draft the RFP. Does that preclude them from responding to the RFP?

Yes.

40. "In reference to XII (Special Terms and Conditions Information Technology), Subsection .13. (No End User agreements), is the role of this provision to clarify

the role of end user agreements not integrated into the agreement?" i.e click-through terms to website...

The executed contract shall reference all the terms and conditions of the contract. Any other agreements or terms and conditions whether electronic, click-through, verbal or in writing, with University employees for other End Users are null, void and without effect, and only the terms of the contract awarded from the IAM RFP shall apply.

41. Clarify if they want 10 individual CDs or flash drives for item 4.

Yes, submit ten (10) individual, unsecured electronic copies of the entire proposal, including all attachments and any proprietary information.

42. We have a partner that we would like to bring into our solution and they are a minority owned company but not yet registered as a SWAM in Virginia. Do we have to have them register ahead of the due date or can that be completed shortly after the November 17<sup>th</sup> due date?

The SWaM's numerical score is for DSBSD registered firms only. If a proposed subcontractor is in the process of completing the registration, the points are only added to the total score after the registration is complete prior to the contract award. The points are not retroactive and are only added at the next milestone scoring during the RFP evaluation for firms that are still under consideration for the contract award. The same rule applies for a prime contractor SWaM firm.

43. Which solution do you use for IaaS and PaaS?

We currently are not working with a IaaS/PaaS. We have a RFP for this solution.

44. Do you have Privilege Access Management in your environment?

No.

45. Are you looking for a solution that will provide access management for VCU Health systems applications?

No, we are looking for a solution to manage VCU application access only. We do create identity for VCU health in our current IdM to provide access to our resources.

46. What are you using for SIEM - Security information and event management?

IBM - QRadar used for event log aggregation and event correlation

47. What are you using for your HR system?

Ellucian Banner - See Page 6 of the RFP.

48. Is your Active Directory integrated with Banner?

NetIQ eDirectory is integrated with Active Directory. Banner is not integrated with Active Directory.

49. Is Federation and SSO included in this RFP?

No, we are interested in the capabilities of the solution but it's not a requirement at this time.

50. How mature is your Role Based Access Management

Very immature.

51. What are using for MFA - Multi Factor Authentication and are you using it for a small subset of your staff?

We are using Duo for MFA. We are using it for staff, faculty and students depending on the service.

52. Ref: PS-PROV-025.....Roles defined in Section XXXX....where is Section XXXX?

Correction: Please refer to Section V. in RFP, 'Statement of Needs' - Key Applications and Systems.

53. How many applications should be included in a Phase 1 solution deployment? (and what are the highest priority, essential applications)

Correction: Please refer to Section V. in RFP, 'Statement of Needs' - Key Applications and systems.

Initial phase will include integration with Flat-file imports, Banner, Google Apps, VCU Card, NetIQ eDirectory, Active Directory, and Database connector.

54. Is an existing solution being replaced? If so, is there any use case, run book or design-level documentation that be shared?

Ref.	Category	RFP Question	Clarification Question	VCU Response
n/a	n/a	n/a	Is an existing solution being replaced? If so, is there any use case,	VCU does not have an identity governance and administration (IGA) solution.



			run book or design-level documentation that be shared?	VCU does have NetIQ eDirectory as an identity store. If your solution plans on replacing eDirectory please be sure to provide details.
--	--	--	--	--

55. Please describe any requirement for workflow-enabled approval functionality in terms of use case, complexity and potential customization to any special VCU needs.

Ref.	Category	RFP Question	Clarification Question	VCU Response
n/a	n/a	n/a	Please describe any requirement for workflow-enabled approval functionality in terms of use case, complexity and potential customization to any special VCU needs	VCU will require standard workflows, such as birthright, role-based, or self-service request, manager approval, entitlement-owner approval (permission-, group-, role-, entitlement-owner, etc.), information security approver, and manual fulfillment or auto-fulfillment.

56. Any requirement for separate distinct UI look-and-feel or branding (colleges, departmental, etc.)?

Separate distinct UI branding for VCU would be preferred but not required at departmental level.



**RFP - Addendum**

DATE: November 2, 2016

ADDENDUM NO. 02 TO ALL OFFERORS:

Reference - Request for Proposals: RFP #7216216JC

Commodity/Title: Identity and Access Management (IAM) Software  
and Services

Issue Date: October 17, 2016

Proposal Due: November 17, 2016 at 11:00 AM

Pre-Proposal Conference: October 31, 2016 at 2:00 PM

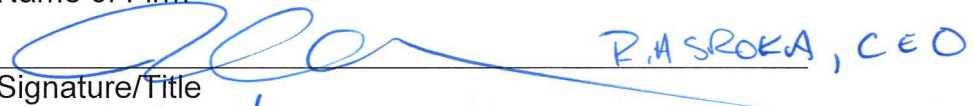
The above is hereby changed to read: **See Attached.**

NOTE: A signed acknowledgment of this addendum must be received by this office either prior to the proposal due date and hour or attached to your proposal. Signature of this addendum does not constitute your signature on the original proposal document. The original proposal document must also be signed.

Very truly yours,

Jackie Colbert  
Procurement Services  
Information Technology Category Manager and Contracting Officer

FISCHER INTERNATIONAL Identity, LLC.  
Name of Firm

  
Signature/Title R. ASROKA, CEO

11/1/2016  
Date

# ***Fischer International Identity***

Identity Management Made for Higher Education™

RESPONSE TO RFP #7216216JC

## **Virginia Commonwealth University**

Identity and Access Management (IAM) Software and Services

November 17, 2016

Attachment G – References and  
Attachment I - Dunn & Bradstreet are confidential

**Gary J. O'Neill**

Sales Director

Phone: (678) 366-0426

Email: [gjo@fischerinternational.com](mailto:gjo@fischerinternational.com)

Fischer International Identity, LLC 9045 Strada Stell Ct.

Naples, FL 34109

Phone: +1 239.643.1500

[www.fischerinternational.com](http://www.fischerinternational.com)

The information contained herein is Fischer International Identity, LLC Confidential and Proprietary. Do Not Distribute without prior written authorization from Fischer International Identity, LLC

# ***Fischer International Executive Summary***

## ***Our Mission “Your Success”***

### **Executive Summary**

Fischer Identity is pleased to respond to Virginia Commonwealth University RFP ##7216216JC for Identity and Access Management (IAM) Software and Services. As you may know, Fischer has a very successful tenure and strong reputation in the Identity and Access Management market, specifically in Higher Education. The Fischer Identity mission is simple: Our mission is “Your Success.” From how the solutions are designed and developed to our implementation methodology, the goal is always focused on driving business value for our customers and to reduce risk in a constantly changing world. Fischer has taken strong strides to minimize unnecessary overhead and cost to our customers. Our policy is to build a partnership while investing in our customers by providing low cost, in many cases no-cost, feature enhancements to help solve your problems. Our post-production Solution Management team is there for you 24 hours a day, 7 days a week, 365 days a year to assist if you ever have issues that need to be resolved.

This is what Fischer Customers experience...

- Solutions are delivered in 8 to 12 weeks after the Statement of Work is completed
- 98% of all customer deployments are successful
- 93% customer retention rates, we rarely lose a customer
- Interoperability platform enables rapid deployments full suite IAM solution either on-premise, cloud systems or hybrid offerings
- No programming and/or customizations: simple configurations drastically reduce the time and skills needed to administer and extend the solution
- Lowest professional services in the market, no follow on Services required
- No-cost, no-services Upgrades

We've long been advocating a product that minimizes the necessity for professional services because we know IAM customers are tired of a high services costs, elongated deployments and significant cost ratios between license and services. At Fischer Identity, we know how to merge a full suite IAM product with an implementation model that lowers the services-to-licensing ratios significantly and drastically speeds the time-to-value for our customers. Our tenure in the IAM market has allowed us to leverage our new concept to avoid the too often failed IAM deployments from other IAM vendors.

Gartner has stated that more than half of all IAM deployments end in failed state. There are multiple reasons why projects fail, or are perceived by the organization to have failed because the program does not end up servicing the long term business objectives and goals the organization. At Fischer Identity we focus on addressing, through product and process, all of the cultural norms that plague legacy IAM deployments and programs. We've been doing what all other vendors are now attempting to do. We can help organizations manage their risk, enable business agility, successfully complete the implementation on-time and within budget as well as provide the lowest TCO in the market.

In summary, we are constantly innovating and evolving our product and fine-tuning our methodology. We are never satisfied because we know we can continue to make it easier. We want every company or institution to have an automated Identity and Access management solution so they can more agile in running their business. Failed IAM implementations are in the past when moving to the Fischer platform. The IAM Evolution has arrived and Fischer Identity is the answer. Why continue to gamble with IAM solutions? Take the second guessing out of your decision making, now is the time.

## **Your Solution**

Fischer will be tasked with creating an Identity Management solution that will provide Password Management, User provisioning, Access Management and integration with target systems such as Google Apps for Work, Banner, Active Directory NetIQ eDirectory, and the physical / badge access.

Users will be provisioned with “birthright” access to ensure they have the correct access on day one. Users will interface with the solution using the Fischer Self-Service portal for requesting access, changing their password and managing their identity profile. Authorized users can also log into self-service to claim their account upon initial provisioning.

Fischer will use Banner as the source of authority for processing users. The solution will deploy role based access to determine what access users should be provisioned with. When a user no longer qualifies for a role their access will be deprovisioned.

The solution will give VCU visibility into what users have access to. This will utilize the Fischer compliance module to allow for reports to be generated and executed as needed. Authorized users will also have the ability to search for users to see what their current access is.

Employees, contractors, students and faculty will be able to reset password by logging into the Fischer Self-Service portal, navigating to the ‘forgot password’ kiosk in order to answer their security questions or they can request a PIN to a mobile device or external email. Once the user has verified their identity they will be able to reset their password, which will be synced to all their applications that are managed by Fischer.

If Virginia Commonwealth decides to purchase Federated Single Sign-On, Fischer will enable SSO for applications that support SAML integration (version 1.0, 2.0 and 3.0). Applications that do not support SAML natively will require further discovery for alternate ways to integrate with the Fischer SSO module.

# Table of Contents

## **Executive Summary**

### **Your Solution**

#### **A1 - Technology Requirements**

#### **A2 – Professional Services**

#### **A3 – Pricing**

#### **A3 – Security of Data**

#### **B – Specific Proposal Requirements**

#### **Appendix I**

#### **Appendix II**

Attachment A: Fischer Implementation Methodology T-IT-071, PS-APP-008 and C-ICD-005.

Attachment B: Fischer Projects Prerequisite Guide T-ARCH-043 and T-IOM-033

Attachment C: Fischer Data Breach Response Policy PS-INTEG-015

Attachment D: Service Organization Control 2 Report T-DG-022 and T-DG-027

Attachment E: Fischer Pricing Methodology and Detailed Quote C-SLC-001, C-SLC-003, C-ICD-008 and C-ICD-009.

Attachment F: Service Level Agreement T-R-037

Attachment G: Fischer References (CONFIDENTIAL) PS-APP-007, PS\_EXP-001

Attachment H: Certificate of Liability Insurance PS\_EXP-001

Attachment I: Dunn & Bradstreet Report (CONFIDENTIAL) PS-EXP-001

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
1	Reference	Category	Question	Answer
2	T-EXP-001	Experience and References	Describe your company's and years in business.	<p>Fischer International Systems Corporation was founded in 1982 (34 years). In 2006, the identity management practice was spun-off, creating Fischer International Identity, LLC (10 years).</p> <p>Fischer is recognized as a pioneer in the information security space and has been first-to-market with multiple solutions and technologies.</p> <p>1980s: 1st PC Security Solution, 1st PC Security product rated by the National Security Center (NSC)</p> <p>1990s: 1st Security Solution for Windows 95 and Windows NT. 1st meta directory on IBM z/OS</p> <p>2000s: 1st SOA-compliant Identity Management Architecture, 1st Provisioning Solution Validated for Oracle / PeopleSoft, 1st Mobile Password Reset and Provisioning Approval Solution, 1st IAM solution to eliminate scripting and programming requirements</p> <p>2010s: 1st Identity Management Solution for SaaS/Cloud delivery</p>

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
3	T-EXP-002	Experience and References	Describe your company's background and history delivering identity and access management (IAM) integration services.	<p>Fischer has a 34 year history bringing security technology innovations to market and has been developing identity management solutions longer than most any other vendor. As the IDaaS market sees new entrants, it is important for VCU to be aware the trickle-down benefits of choosing a Partner that can offer proven solutions and implementation processes. With 15 years of experience delivering identity management solutions to customers, ten of which include IdM as a cloud-based service, we have refined our product, services and delivery model so that our customers can more easily and cost-effectively attain their goals. This is what being a Partner is all about; being maniacally-focused on our customer's satisfaction and success.</p> <p>IdM Replacement &amp; Transition Approach: Fischer's deployment approach and methodology are aimed at success. We understand that a successful solution is more than a "regurgitation" of our customer's business requirements into a new platform. We understand that there is much more to providing a complete solution than the business requirement. Although the business requirement is at the heart of every solution we provide, we put extra focus on security, and procedure to give our customers the confidence that we understand the importance of the function we provide to our customers, especially our hosted customers. Fischer has very specific opinions on how to best transition a customer's existing IdM environment. We follow a proven, phased approach that ensures short-term value and relies heavily</p>



Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
4				<p>on customer participation. Starting with Discovery, we obtain a "lay of the land" regarding the services you're currently providing vs. those that you want to provide (and how). Prioritization follows by determining criticality of each service based on multiple scored variables, e.g., user-facing, business criticality, risk/vulnerability, compliance/audit deadlines, etc. A Review phase ensues allowing the customer to see the project in totality and (re)consider the criticality of some processes, whether a process might be best implemented using the vendor's out-of-the-box approach vs. remodeling the existing process, etc. The Scheduling phase then begins and both Fischer and W&amp;L will begin working to plan, including Sprint planning (agile process). Proposed Solution: Based on W&amp;L's requirements, we are proposing Fischer Identity Suite™ and Fischer Federated SSO in the hosted model: Hosted environment: The solution operates in a Virginia-based Rackspace facility that satisfies the requirements of both the ISAE 3402 and SSAE 16 and is an SOC Type 2 facility.</p> <p>Connected Systems/Integration: JCU target and source of authority systems Ellucian and Active Directory are supported. Fischer has approximately 100 out-of-the-box connectors available. If a connector is not available out of the box, Fischer has Command Line Connectors, Data Base Connectors and LDAP Connectors which can be used to connect to the back end of different services. Fischer will work with W&amp;L to build the integration.</p> <p>Role Management &amp; Provisioning: Fischer has extensive</p>

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
5				<p>role management &amp; provisioning. Fischer has extensive experience with provisioning and will work with you to define your policies and procedures related to W&amp;L access policies. Fischer is also known for its ability to easily handle any number of affiliations a person may have within your institution. Fischer supports the RBAC structure and provides further granularity to enable ABAC (attribute based access control) to allow W&amp;L to further qualify access based on any person attribute it chooses.</p> <p>Credential Management (a.k.a. Password Management): Fischer provides multiple mechanisms to empower users to manage their own passwords, as well as a help desk layer to provide an interface for support personnel to view and interact with the end user's identity and associated account information.</p> <p>Federated SSO: Fischer's virtual IdP service removes the burden on customers to manage a federated infrastructure yet still maintain a local authentication presence to ensure credentials remain stored behind the firewall.</p>
6	T-EXP-004	Experience and References	Describe your company's status as an authorized reseller, or authorized partner of the technology vendor.	<p>Fischer has performed over 90% of all implementations. We work with a small number of integration partners that share our commitment to our customer's success, have proven their ability to successfully deploy our solution and adhere to our standards of excellence.</p>

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
7	T-EXP-005	Experience and References	What differentiates your company from its competitors for Technology solution?	<p>Culture: The biggest difference is our Culture; it drives every decision we make. We're customer advocates and propeller heads, meaning that we listen to our customers and are very good at creating solutions that meet customer needs. And that's very apparent in our solutions; we've taken a completely different approach to managing the Identity Lifecycle so customers are able to secure more parts of the campus with less effort and cost, start benefiting from the solution in weeks vs. years, minimize or eliminate professional services, and quickly respond to changes. Our company has been structured to ensure that we strive to meet customer expectations every day: deployment times, technical support, licensing, product roadmap, etc.</p> <ul style="list-style-type: none"> <li>- Higher education specialization. We understand higher education processes, systems/technical environments, users, business challenges, goals, and missions.</li> <li>- Choice of Deployment Model: on-campus software or hosted cloud subscription</li> <li>- Ease and Speed to change and extend the solution to meet new business requirements.</li> <li>- Experience: Fischer has 30-year history in information security and has been developing identity management solutions since before the sector was called "identity management."</li> </ul> <p>Full time equivalent student license model: license fee is</p>

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
8				<p>Full-time equivalent student license model, license fee is based on FTES enrollment count, yet provides licenses for 10-times that number so that institutions can service more user populations without adding cost.</p> <p>- Guaranteed Implementation Time and Cost: Deployment cost is locked BEFORE the solution is purchased; Fischer will pay the customer a penalty fee for every day the project is late* (terms apply).</p> <p>- Minimal Professional Services. Ease of implementation minimize costs.</p> <p>- Time to value: Fischer is setting unprecedented deployment times as a result of "configuration vs. customization" approach, Agile project methodology, and strong project management. Reference:  <a href="http://campustechnology.com/articles/2014/09/24/missouri-college-overhauls-identity-management-system.aspx">http://campustechnology.com/articles/2014/09/24/missouri-college-overhauls-identity-management-system.aspx</a></p>
9	T-EXP-007	Experience and References	Please provide five (5) reference accounts where you implemented this particular technology solution. Two (2) of these references should include user / identity populations over eight-thousand five hundred (8500). Please indicate which references are higher education if any.	Please see Attachment G - References.
10	T-AC-101	Access Certification	Can the solution create certifications for individual entitlements, such as group memberships, and assign them to the appropriate data owners?	When business workflows change, Fischer provides point and click and drag and drop functionality so change management does not have to become an overwhelming exercise.
11	T-ADM-306	Administration Configuration	Does the solution allow business / process owners to modify workflow behavior without having to modify code (e.g., change approver on a role or entitlement)?	When business workflows change, Fischer provides point and click and drag and drop functionality so change management does not have to become an overwhelming exercise.

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
12	T-ADM-307	Administration Configuration	Does the solution provide a graphical user interface for defining and managing identity business processes and workflows?	Fischer provides a pre-packaged self service UI for end users for everything from password reset to profile management, including help desk functionality and resource requests and approvals. The Fischer administrative UI provides all the screens necessary to configure and manage profiles, approval workflow schedules, compliance, auditing, reporting, etc.
13	T-ADM-309	Administration Configuration	Does the solution allow customization of workflows to meet the unique needs of a deployment?	Workflows may be customized as much as is necessary to meet unique deployment requirements.
14	T-ADM-313	Administration Configuration	Does the solution provide inline, GUI-based rule editing to allow for rapid definition or editing of configuration rules?	Fischer Identity is a GUI-based product where all configurations can be performed via point and click.
15	T-ADM-314	Administration Configuration	How are customizations and configurations rolled forward in an upgrade?	Identity as a Service® cloud customer administration is managed by Fischer International Identity's support team. Custom configurations are backed up and after the upgrade is installed, they are re-applied.

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
16	T-ADM-315	Administration Configuration	Does the solution externalize authentication, such as single sign-on (SSO), SAML 2.0, or pass-through authentication such as LDAP or integrated windows authentication (IWA)?	<p>Fischer Identity will be configured to utilize whatever authentication mechanisms are appropriate for a given application. In many cases, access to an application is granted through membership in an AD/LDAP group, in which case Fischer's provisioning policies will be configured to grant group membership to authorized users. Applications which require an internal user ID and password will be configured for provisioning of such to the application or system with password management and synchronization capabilities out of the box.</p> <p>Fischer provides an integrated Federated SSO IDP, based on Shibboleth, for those applications which are capable of accepting a SAML login. Fischer's approach to Federated SSO is somewhat different in having the IDP integrated with the IDM solution, allowing for tight control over the configuration and release of user attributes to downstream Service Providers and enhanced security through administrative credential management coming from encrypted credentials in the IDM system instead of preconfigured credentials in clear text in the IDP configuration files. Fischer's IDP will only release those user attributes to a downstream SP which have been configured in the SP definition. Those attributes are managed by and derived from the IDM system and the user's identity profile. Fischer Identity is an InCommon affiliate.</p>

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
17				<p>Fischer's IDP may be configured to front-end authentication to CAS and ADFS services for SSO integration of non-SAML targets, such as Microsoft products which rely heavily on ADFS for SSO functionality. In this way, all SSO functions can be incorporated into one user-facing solution.</p> <p>Fischer has developed a plugin for Active Directory which provides a seamless and true single sign-on experience for Windows desktop users. The SSO IDP can determine whether a user is connecting from behind the firewall or not. External users will be prompted for authentication by the IDP as expected. Connections from internal users trigger a query of the AD plugin as to whether the user has an active AD session through a Windows Gina login. If the user has already authenticated through a desktop logon, the IDP will not prompt the user for any further authentication unless required by policy, such as a second factor of authentication, providing a true clientless Single Sign-On capability.</p> <p>Fischer's self-service interfaces fully support SAML and CAS SSO login processes out of the box.</p>
19	T-AR-198	Access Requests	Does the self-service access request solution allow for adding, changing, and removing access from the same interface?	Yes, requirement met out-of-the-box (OOB)
20	T-AR-199	Access Requests	Can the solution facilitate requesting of roles, entitlements, and/or accounts?	Fischer has a policy engine capable of Role Based policy evaluation of users based on Source of Authority events. Fischer also has a robust Self-Service module for Requests that can be used for Requesting and Removing access from users. Approvals can be tied into the request feature if required.

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
21	T-AR-200	Access Requests	Does the solution scope who can request access for others?	Fischer provides native delegation out of the box. We call it "OBO" or On-Behalf-Of, which enables users to take actions on behalf of others. Authorization for this privilege can be provided automatically in the form of a role or user group configuration (i.e. a user qualifies for the role or group and is able to take delegative actions), or manually via an administrative console as needed.
22	T-AR-202	Access Requests	Does the solution enable the user to track access requests made by them and for them?	Self-Service Access Request - Enables users to request access to account and drive approval process through an intuitive portal - without Help Desk calls. Users are presented with only the accounts which they are authorized to select, ensuring that the "principle of least privilege" is always enforced. All access request events are fully audited, from request to approval. Authorized users may also request access on behalf of other users, such as contractors or vendors.
23	T-AR-204	Access Requests	Does the solution support configurable workflows to manage self-service access requests/changes?	Yes, Fischer Identity supports configurable workflows to manage self-service access requests/changes. Our workflow engine is where we truly differentiate ourselves from the competition. We have abstracted the coding layer and require only a script-based approach to building workflows. You do not need to be an expert in any one programming language, rather we have normalized the skillset required to build enterprise grade identity management workflows. Our studio provides point and click, drag and drop WYSIWYG usability to build complex workflows without compiling code, understanding a specific library framework, including libraries, defining functions, associated parameters, etc. Fischer has removed the heavy lifting from this layer of the IAM stack and has accomplished an approach to streamline the workflow design and configuration process.



Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
24	T-AR-205	Access Requests	Does the solution give end users a business-friendly dashboard to view status of pending and completed requests?	Yes, we provide multiple interfaces to track the status of requests. The requester has a status view, approval authorities have a queue of pending requests, and administrators can view all of the above plus more details pertaining to the overall process from the admin ui.
25	T-ARCH-040	Architecture Requirements	Is the solution available as Software as a Service (SaaS), also known as Identity as a Service (IDaaS)?	Fischer supports both on-premise and hosted IAM software delivery models. This response provides pricing, support, installation and training for both models.
26	T-ARCH-040-1	Architecture Requirements	Is the solution available as a hybrid deployment, leveraging a mixture of integrated, on-premise, private and/or public cloud?	Yes, the solution can be built as a hybrid deployment.
27	T-ARCH-043	Architecture Requirements	For supported off-premise SaaS, IDaaS, PaaS or IaaS deployments, what does the on-premise infrastructure and application integration look like, such as on-prem Active Directory and other apps?	Please see Attachment B - Official Project Pre-Requisites Guide
28	T-ARCH-044	Architecture Requirements	For supported off-premise SaaS, IDaaS, PaaS or IaaS, deployments what features are not available for each type as compared to the on-prem solution?	The Product features are the same for both IaaS and On-Premise solutions.
29	T-ARCH-061	Architecture Requirements	Does this system provide native compatibility for the following database architectures SQL, Oracle or additional database support?	The product platform supports Oracle, MSSQL and postgreSQL. The product integrates with Oracle, MSSQL, MySQL, DB2, Progress.
30	T-ARCH-062	Architecture Requirements	Is the application optimized for mobile device support including a responsive user interface or app? What is supported out of the box?	We provide self-service functionally via the mobile device. This includes users managing their password and security questions, and approval authorities have the ability to take action from our mobile client. No administrative capabilities are available via our mobile client.
31	T-CR-004	Compliance Requirements	What actions and events are logged?	Runtime errors are logged into multiple distinct log files depending on the scope (for example we log all db queries to a db trace log, all policy transactions to a policy log, etc.). We support Info, Debug and All log levels. Logs are accessible via the admin UI or they are available on the server.
32	T-CR-006	Compliance Requirements	Do you have any data privacy accreditation?	Our data center is an SSAE16 SOC 2 Type II data center.

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
33	T-DAC-278	Data Aggregation and Correlation	What are all the file import options/types that are supported?	CSV, ExcelSheets, Excel (*.xlsx), LDIF, WordTable (*.docx), XML
34	T-DAC-279	Data Aggregation and Correlation	Does the solution support delta reconciliation to rapidly reconcile only new or changed accounts from target resources?	Yes, requirement met out-of-the-box (OOB).
35	T-DAC-282	Data Aggregation and Correlation	Can the application derive the employee/manager relationship from an authoritative identity source, such as the central HR application?	Yes, requirement met out-of-the-box (OOB).
36	T-DAC-283	Data Aggregation and Correlation	Can the application support multiple authoritative sources for identity data?	Fischer can pull from one or multiple authoritative sources, and execute business logic to build netid's and email addresses per your naming convention. Fischer integrates with potentially hundreds of systems and can provide downstream target provisioning as well as push information back to upstream authoritative data providers.
37	T-DAC-290	Data Aggregation and Correlation	Does the solution support associating contextual metadata with each entitlement (business-friendly description, data owner, account type, privileged account, system account, etc.)?	Yes, Fischer identity supports this requirement.
38	T-DAC-293	Data Aggregation and Correlation	Does the solution support importing and evaluating activity data (e.g., SIEM feeds and application log files) from target systems?	Third-party product utilized to meet this requirement.
39	T-DAC-297	Data Aggregation and Correlation	Can the solution support collecting data from SaaS applications (e.g., Google Apps for Education, Office 365, Salesforce.com, etc.)?	Yes for Google Apps for Education and Office 365.
40	T-DEP-299	Deployment	Does the solution support running on virtual machines/servers?	Fischer can run all layers of the IAM stack on virtual servers.
41	T-DEP-301	Deployment	How are product configurations and customizations migrated between environments (development, test, staging, production)?	We provide an import / export feature that allows for simply portability of the solution between environments.
42	T-DEP-302	Deployment	Can applications run in a clustered environment for load balancing and/or fail-over purposes?	Yes, requirement met out-of-the-box (OOB).
43	T-DG-022	Data Governance	Please describe the data validation controls that are in place to that ensure the correct type, the completeness and the accuracy of data stored within this system.	Please see Attachment D - SOC 2 Report.

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
44	T-DG-025	Data Governance	Is the data provided real-time, or through periodic updates? What frequencies are available?	Fischer's workflows can be designed in multiple ways to fit the customer's specific architectural and business requirements. Triggers are available if the customer wants real-time event detection. We've typically found that near-real-time processing of Banner information provides a more predictable downstream provisioning process. Since triggers are prone to losing data, a controlled delta export process is a much more stable approach. This process will be scheduled to run at whatever time interval the customer requires and it's job is to determine what changes occurred from the previous execution. The process will determine what has changed (added/modified/deleted). Again, Fischer can support triggers if the customer desires them. Once records are received from the source of authority, Fischer will evaluate the records against a set of defined organizational provisioning and security policies. The result is either a qualification or disqualification of a source of authority user to/from the downstream target systems. Typically user types such as student, faculty, staff, graduate, alumni, etc. are used to determine which systems a user will gain access to, as well as which password policy the user must adhere to.
45	T-DG-026	Data Governance	Please describe the solutions data retention configuration options for audit logs, configurations, entitlements, identities and other relevant data.	All incident data is stored within our ticket system. The incident ticketing system is only accessible by approved users within Fischer and requires a UserID and Password in order to access. Items that are used for problem diagnosis and troubleshooting, i.e. solution logs, server logs are only accessible to Fischer staff that require this level of access and require the Fischer user to enter login credentials in order to access.

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
46	T-DG-027	Data Governance	Please describe the process for detecting and preventing the unauthorized modification, update, or deletion of records within the system.	<p>Fischer hosts its Identity as a Service infrastructure in Rackspace's SSAE-16 SOC2 Type II compliant data centers. Included with this service is intrusion prevention and initial incident response. A copy of this SSAE-16 attestation will be made available upon request.</p> <p>Fischer follows industry standard secure software development and testing methodologies in its development processes. Periodic vulnerability assessment is performed. Please see Attachment D-SOC 2 Report.</p>
47	T-DG-028	Data Governance	Does your system provide for export of customer data?	Only authorized Fischer personnel are able to view enterprise data in a cloud based solution. Data can be exported to the client if circumstances dictate and allowed by client security policies.
48	T-FR-096	Functional Requirements	Please describe the flexibility and configurability the system UI, and explain how functional configurations are propagated and maintained throughout the system.	If the system is hosted, Fischer will manage all of the configurations in the hosted environment; these configurations are based on VCU requirements.
49	T-G-333	Growth	What are your customer's options should they decide to change deployment architectures at a later time (on-premise, Hybrid, private cloud, public cloud, PaaS, SaaS/IDaaS, etc.)?	<p>We provide for the ability to export the solution and provide all data, which includes configuration, identity information as well as the audit trail in the form of an XML bundle. This bundle can be parsed and used to load another system if the University were to make the unfortunate decision to terminate services with us.</p> <p>Resumption of self-support would work the same way. We have moved a customer from our cloud data centers to on premise in a weekend. It is a very straight forward process.</p>

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
50	T-IAI-256	Identity and Access Intelligence	Can pre-defined reports be personalized by end users to fit their specific business needs?	Fischer Identity records all logins to the Fischer Identity self-service, administrative, and Federated SSO portals, along with extensive other activities. These records are stored in the Fischer Identity audit logs and are accessible through approximately 100 out of the box reports plus custom configured reports. In an on-premise implementation, the customer may also run SQL queries against the audit database directly, if required.
51	T-IAI-262	Identity and Access Intelligence	What pre-defined reports are provided, and which reporting customization features are provided (scheduling reports, on-screen, downloadable, emailed, PDF, Excel, CSV, etc.)?	Fischer provides an accessible audit store that contains information about all actions and activities that occur within the platform. Fischer is able to log this information for our native application as it relates to authenticating to the interfaces, and tracking and detecting policy violations through various compliance and governance mechanisms. Compliance assessments can be executed on a scheduled basis to find (report) all access control policy violations and present audit controllers with remediation options as well as override options, including access certification.  The audit store is a well-organized database that is queried from Fischer's native reporting interface, or externally from third party reporting tools like Crystal (or direct DB queries). There are approximately 100 out-of-the-box reports available plus the ability to create custom reports covering all aspects of the platform in a multitude of views. Reports can also be scheduled to run periodically and notify concerned auditors when complete. Auditors can login into self-service portal to view the reports. The reports are downloadable and can be emailed. Reports can be exported in Excel and .csv format.
52	T-IOM-033	IT Operations Management	Please describe any recommended system requirements for this system.	Please see Attachment B - Official Project pre-Requisites Guide.

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
53	T-IOM-035	IT Operations Management	Please describe what standard automation and workflow process are provided standard without customization, as well extensibility through APIs.	<p>Fischer provides out-of-the-box connectors for the following systems and applications for SaaS, hosted and traditional on-premise environments:</p> <p>Common/Core Systems</p> <ul style="list-style-type: none"> <li>• All systems and applications that support SPML v2</li> <li>• All systems and applications that support web services</li> <li>• All systems and applications authenticated by an LDAP server</li> <li>• All systems and applications authenticated by JDBC database</li> <li>• All systems and applications authenticated by Microsoft Active Directory</li> </ul> <p>Operating Systems / Authentication Systems including:</p> <ul style="list-style-type: none"> <li>o AIX</li> <li>o HP-UX</li> <li>o IBM 4690 Operating System</li> <li>o Linux</li> <li>o Microsoft Windows (2008, 2003, 2000) - (including deep folder permissions)</li> <li>o Microsoft Windows Command Line</li> <li>o MIT Kerberos</li> <li>o Novell NetWare - (including deep folder permissions)</li> <li>o RSA Authentication Manager</li> <li>o RSA SecurID</li> <li>o SCO UNIX</li> <li>o SQL Stored Procedures</li> <li>o Sun Solaris (with NIS, NIS+, directory authentication or</li> </ul>

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
54				<p>SSH)</p> <ul style="list-style-type: none"> <li>o UnixSSH</li> <li>o z/OS and OS/390 including subsystems: TSO, CICS, IMS-DC, etc. (RACF, ACF2 and Top Secret)</li> </ul> <p>Directories</p> <ul style="list-style-type: none"> <li>o Microsoft Active Directory (ADSI) - (including deep folder permissions)</li> <li>o Microsoft Active Directory Lightweight Directory Service (LDS) (formerly called ADAM)</li> <li>o Novell eDirectory</li> <li>o Novell Directory Service (NDS)</li> <li>o Sun Java System Directory Server, Sun ONE, iPlanet (now called Oracle Directory Server)</li> <li>o Oracle Internet Directory</li> <li>o IBM Tivoli Directory</li> <li>o CA Directory</li> <li>o Siemens DirX</li> <li>o 389 Directory (formerly called Fedora)</li> <li>o Red Hat Linux Directory</li> <li>o Open LDAP Directory</li> <li>o All other LDAP v3 directories</li> </ul> <p>Databases</p> <ul style="list-style-type: none"> <li>o Oracle Database</li> <li>o MS-SQL Server</li> <li>o MS A</li> </ul>

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
55				<ul style="list-style-type: none"> <li>o MS-Access</li> <li>o IBM DB2 Database</li> <li>o IBM Ingres Database</li> <li>o MySQL</li> <li>o Sybase Database</li> <li>o Informix Database</li> <li>o PostgreSQL Database</li> <li>o Progress Database</li> <li>o All other JDBC databases</li>   <li>Oracle E-Business Suite including:</li> <li>o Procurement</li> <li>o Contracts</li> <li>o Performance &amp; Daily BI</li> <li>o Customer Data</li> <li>o Customer Relationship</li> <li>o Financials</li> <li>o HR</li> <li>o Interaction Center</li> <li>o Learning</li> <li>o Logistics</li> <li>o Maintenance</li> <li>o Manufacturing</li> <li>o Marketing</li> <li>o Order</li> <li>o Product Lifecycle</li> <li>o Projects</li> <li>o Sales</li> <li>o Service</li> <li>o Supply Chain</li> </ul>



Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
56				<ul style="list-style-type: none"> <li>o Supply Chain</li> <li>o Transportation</li>   <li>Oracle-PeopleSoft - all applications including:               <ul style="list-style-type: none"> <li>o Asset Lifecycle</li> <li>o Campus Solutions</li> <li>o CRM</li> <li>o Enterprise Performance</li> <li>o Enterprise Service Automation</li> <li>o Financials</li> <li>o HCM</li> <li>o Supplier Relationship</li> <li>o Supply Chain</li> <li>o Enterprise Tools &amp; Technology</li> </ul> </li>   <li>SAP R/3 Enterprise and SAP NetWeaver (ABAP) applications including:               <ul style="list-style-type: none"> <li>o SAP Business Suite</li> <li>? SAP Customer Relationship Management</li> <li>? SAP ERP</li> <li>? SAP Product Lifecycle Management</li> <li>? SAP Supply Chain Management</li> <li>? SAP Supplier Relationship Management</li> <li>o SAP Human Capital Management</li> <li>o SAP Manufacturing</li> <li>o SAP Service and Asset Management</li> <li>o Alloy</li> <li>o Duet</li> <li>o Duet Enterprise</li> </ul> </li> </ul>

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
57				<ul style="list-style-type: none"> <li>o SAP BusinessObjects analytic solutions</li> <li>o SAP BusinessObjects business intelligence solutions</li> <li>o SAP BusinessObjects GRC solutions</li> <li>o SAP BusinessObjects EPM solutions</li> <li>o SAP Crystal solutions</li> <li>o SAP solutions for auto-ID and item serialization</li> <li>o SAP solutions for enterprise information management</li> <li>o SAP solutions for sustainability</li> <li>o Solution extensions</li>   <li>Help Desk / CRM / Service Center applications including:               <ul style="list-style-type: none"> <li>o Atlassian JIRA</li> <li>o Microsoft Dynamics CRM and IFD</li> <li>o Salesforce.Com</li> </ul> </li> <li>• SSO and Federation including:               <ul style="list-style-type: none"> <li>o Entrust GetAccess</li> <li>o Imprivata OneSign</li> <li>o RSA ClearTrust</li> <li>o Tivoli Access Manager</li> <li>o Tivoli Federated Identity Manager</li> </ul> </li>   <li>Email including:               <ul style="list-style-type: none"> <li>o Microsoft Exchange</li> <li>o Lotus Domino / Notes (web client and Windows Client ID files)</li> <li>o Novell GroupWise</li> <li>o Fischer InterPost</li> <li>o Fischer TAO</li> <li>o IMAP servers</li> </ul> </li> </ul>

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
58				<ul style="list-style-type: none"> <li>o LDAP-compliant email systems</li> <li>o Microsoft Exchange Pagers</li> <li>o Zimbra</li> <li>o POP servers</li>   <li>Other applications including:</li> <li>o Accenture ITSM Remedy</li> <li>o AccPacc Pro</li> <li>o Blackberry Enterprise Server (BEIS)</li> <li>o Blackboard</li> <li>o Canvas LMS</li> <li>o Cerner Millennium Suite (approximately 50 healthcare applications)</li> <li>o Desire2Learn</li> <li>o Duo Security (two-factor authentication)</li> <li>o Google Applications</li> <li>o IBM 4690 Supermarket Application</li> <li>o Live@EDU</li> <li>o Luminis (through BEIS)</li> <li>o Microsoft Office365</li> <li>o Moodle</li> <li>o RCMS</li> <li>o SagePro (ERP)</li> <li>o Sakai</li> <li>o ServiceNow</li> <li>o Sungard Banner</li> <li>o WebEx</li>   <li>Flat files including:</li> <li>o CSV</li> </ul>

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
59				<ul style="list-style-type: none"> <li>o Excel</li> <li>o LDIF</li> <li>o Word</li> <li>o XML</li> </ul> <p>This list is continually growing as new integration methods are included in the product.</p>
60	T-ISI-321	IT & Security Integrations	Can the solution integrate with privileged access management systems? Which systems are supported?	Fischer's PAM, called High Privileged Account Management (HPAM) can work with any connector that is available out of the box that supports password management. There are no prewritten connectors for other external PAM systems, though existing generic integration methods may be applicable.
61	T-ISI-323	IT & Security Integrations	Does the solution integrate with security information & event management solutions? Is QRadar supported?	Fischer WebSSO solution is built on a Shibboleth IdP version 3.x stack and supports any protocols supported by the current IdP 3.x release. Fischer also supports integration with additional multi-factor authentication protocols outside of the official Shibboleth supported ones.

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
62	T-ISI-324	IT & Security Integrations	What applications, systems and platforms to you provide out-of-the-box connector support for, and describe the granularity of entitlements that can be managed and gathered?	Fischer Identity includes connectors for many specialized systems and cloud services (See answer to question T-IOM-035 above). In addition, Fischer's robust generic database, LDAP, and web services connectors allow for connectivity to many more systems that do not require the development of specialized connectors. If required, Fischer will develop up to three (3) connectors to commercially viable off-the-shelf applications at no additional cost, providing such new connectors are applicable to the majority of the Fischer customer base. Custom connectors for in-house applications can be developed for a fee.
63	T-ISI-329	IT & Security Integrations	Which common protocols or interfaces can be extended for custom connectors (SOAP, REST, SCIM, LDAP, JDBC/ODBC, etc.)?	Fischer supports import via SOAP and SPML and export via REST. Modifications of user data is available using REST. Fischer also has the ability to update any number of attributes in target systems we have a connector for or where we can use a JDBC connection to. We do not currently have a SCIM interface; SCIM is on our roadmap.
64	T-ISI-330	IT & Security Integrations	Does the solution expose APIs and Web Services so that it can be extended? Which functions are exposed? Which functions are not exposed?	Fischer Identity supports this requirement. The solution has a published set of REST API 's.
65	T-ISI-331	IT & Security Integrations	What tools and facilities are provided for developing custom connectors to custom interfaces?	Fischer provides extensive documentation and sample files for developing integration with internally developed applications. Fischer Identity is a Java application, so a competent Java developer should be engaged for connector development.  Fischer should be contacted for integrations with commercially viable off-the-shelf applications, which will usually be developed at no cost and offered as standard integration methods in future releases.
66	T-ISI-332	IT & Security Integrations	Describe the level of effort, and skillsets required, to develop a custom connector?	Fischer Identity is a Java application, so a competent Java developer should be engaged for connector development.

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
67	T-LM-210	Lifecycle Management	Does the solution provide visibility to access changes initiated through automated change events — e.g., new hire, promotion, termination?	Yes, requirement met out-of-the-box (OOB).
68	T-LM-211	Lifecycle Management	Does the solution support delegation of approval requests to other users within the system and is this information tracked and audited?	Fischer Identity can be configured to delegate approval requests to other users within the system. Approvers may temporarily delegate their approval authority to others in two ways. One is to delegate it to a specific person for either a specified or indeterminate time period, and they can delegate only new requests or all requests in their queue plus new ones. The other method is to place themselves into an "Unavailable" status, in which case they will not see new requests and all requests will automatically escalate. All transaction within the Identity solution are audited.
69	T-LM-214	Lifecycle Management	Can the solution automatically determine the need to create new accounts associated with adding entitlements and roles?	Fischer Identity can automatically add/change/ revoke user access to IT and physical assets based on real-time events (e.g., matriculation, new hire, furlough) and self-service requests all in compliance with your policies.
70	T-LM-215	Lifecycle Management	Can the solution request additional information from users involved in the access request process — e.g., requester, approver, application/data owners?	Yes, request process and corresponding UIs are customization from administration UI. Coding is not required to meet vast majority of requirements.
71	T-LM-217	Lifecycle Management	Does the solution support tracking and reporting on service-level metrics?	Yes, requirement met out-of-the-box (OOB).

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D															
72	T-MS-081	Software Maintenance and Support	What is the standard SLA for each level of support? What are the defined incident severity levels and the corresponding SLAs? Please describe your escalation process?	<p>Fischer provides a web-based support portal for customers to report incidents, solution change requests, and inquiries. Within the portal, customers have the ability to set the priority level of support tickets. All requests are to be handled within the SLAs. If for any reason, you are not satisfied with the level of service that is provided, the Director of Operations serves as the escalation point. Additionally, a dedicated Fischer executive escalation distribution list can be used at any time to communicate any concerns.</p> <p><i>Table 2: Fischer Escalation for Support Requests</i></p> <table border="1"> <thead> <tr> <th>Priority</th> <th>Criteria for Escalation Within Fischer</th> <th>Notification to</th> </tr> </thead> <tbody> <tr> <td>Priority 1 (Critical)</td> <td>Every 2 hours from time of creation or last update</td> <td>1. Director of Operations 2. Support Manager 3. Primary Support Specialist</td> </tr> <tr> <td>Priority 2 (High)</td> <td>Every 4 hours from time of creation or last update</td> <td>1. Support Manager 2. Primary Support Specialist</td> </tr> <tr> <td>Priority 3 (Medium)</td> <td>No Response to Licensee (which may include plans for a Workaround or a Fix in the next release) has been communicated to Licensee within 1 business day.</td> <td>1. Support Manager 2. Primary Support Specialist</td> </tr> <tr> <td>Priority 4 (Low)</td> <td>No Response to Licensee (which may include plans for a Workaround or a Fix in the next release) has been communicated to Licensee within 1 week.</td> <td>1. Support Manager 2. Primary Support Specialist</td> </tr> </tbody> </table>	Priority	Criteria for Escalation Within Fischer	Notification to	Priority 1 (Critical)	Every 2 hours from time of creation or last update	1. Director of Operations 2. Support Manager 3. Primary Support Specialist	Priority 2 (High)	Every 4 hours from time of creation or last update	1. Support Manager 2. Primary Support Specialist	Priority 3 (Medium)	No Response to Licensee (which may include plans for a Workaround or a Fix in the next release) has been communicated to Licensee within 1 business day.	1. Support Manager 2. Primary Support Specialist	Priority 4 (Low)	No Response to Licensee (which may include plans for a Workaround or a Fix in the next release) has been communicated to Licensee within 1 week.	1. Support Manager 2. Primary Support Specialist
Priority	Criteria for Escalation Within Fischer	Notification to																	
Priority 1 (Critical)	Every 2 hours from time of creation or last update	1. Director of Operations 2. Support Manager 3. Primary Support Specialist																	
Priority 2 (High)	Every 4 hours from time of creation or last update	1. Support Manager 2. Primary Support Specialist																	
Priority 3 (Medium)	No Response to Licensee (which may include plans for a Workaround or a Fix in the next release) has been communicated to Licensee within 1 business day.	1. Support Manager 2. Primary Support Specialist																	
Priority 4 (Low)	No Response to Licensee (which may include plans for a Workaround or a Fix in the next release) has been communicated to Licensee within 1 week.	1. Support Manager 2. Primary Support Specialist																	
73	T-MS-085	Software Maintenance and Support	Please enumerate the various types of support (phone, chat, online, forums, knowledge base, etc.) and the corresponding availability of these types of support based on the support levels available.	<p>Fischer provides a web-based support portal for customers to report incidents, solution change requests, and inquiries. Within the portal, customers have the ability to set the priority level of support tickets. All requests are to be handled within the SLAs. If for any reason, you are not satisfied with the level of service that is provided, the Director of Operations serves as the escalation point. Additionally, a dedicated Fischer executive escalation distribution list can be used at any time to communicate any concerns.</p>															

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
74	T-MS-087	Software Maintenance and Support	How is availability tracked and reported in this system? Does the system provide period reporting on uptime?	Solution availability reports and historical support incident metrics are available upon request.
75	T-MS-091	Software Maintenance and Support	Please describe your backwards compatibility for previous versions of system integrations, and for preserving product customizations, extensions and configurations.	There are multiple components that are a part of our configuration. We've had customers leverage version control systems against the core business logic (stored in XML). Other components are audited and reports can be used to ascertain previous configurations. Fischer does not provide this type of documentation.
76	T-MS-092	Software Maintenance and Support	How many revisions from current product are you still supporting?	<p>Fischer currently supports 3 major releases.</p> <p>Annual software maintenance includes bug-fixes, minor releases and major releases for licensed software and technical support. Fischer generally provides one to two product releases per year in addition to maintenance packs to address specific issues, and service packs that are a combination of maintenance packs and additional features or enhancements to the overall solution.</p> <p>Maintenance is required in both the on-campus and Identity as a Service® (IaaS®) models. The IaaS model also includes services for the daily care and feeding of the IaaS® infrastructure and core solution software.</p> <p>Fischer regularly adds new features based on customer enhancement requests and feedback of customers and partners. When enhancements are added to the product, they are added for all Fischer customers, rather than as customizations delivered only to the requesting customers. This approach enables all customers to benefit from new features and improves support as Fischer doesn't need to track and maintain numerous customized versions. Customers request enhancement through technical support and Fischer conducts regularly scheduled meetings to address the requests.</p>



Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
77	T-PA-268	Platform and Architecture	Does the solution use standard programming language for the customization?	Yes. Javascript, XHTML and Java.
78	T-PA-269	Platform and Architecture	Does the solution support integration with 3rd party applications via web services? (REST, SPML)?	Yes.
79	T-PA-271	Platform and Architecture	Does the vendor support and participate in standards efforts around identity management interoperability (e.g., XACML, SPML, SCIM)?	SPML is supported, SCIM is on our roadmap. We currently do not support XACML.
80	T-PA-272	Platform and Architecture	Does the solution provide pass-through authentication, leveraging existing authentication mechanisms to authenticate users?	Yes, requirement met out-of-the-box (OOB).
81	T-PA-273	Platform and Architecture	Describe the role-based authorization capabilities of the proposed solution. Does it support definition of user roles and assignment of internal access rights based on roles? Can the internal authorization model be customized?	Role based access can be configured per the business requirements of the Client. The client will need to provide the business rules and what access/resources each should get. Then this can be configured within Fischer using its configuration hub to set up your role-based solution.
82	T-PASS-219	Password Management	Are the end-user password management user interfaces integrated with the solution's access request user interfaces for a seamless user experience?	Yes, requirement met out-of-the-box (OOB).
83	T-PASS-220	Password Management	Does the solution provide an option to help users reset forgotten passwords with a Windows desktop (i.e., GINA or Credential Provider plugin)?	Fischer supports this capability by providing the user with a self-service kiosk to reset their forgotten password. Both user-defined email accounts and SMS devices are able to be notified and leveraged for the resetting process. Users also have an option of "Forgot User ID" which enables them to retrieve their ID if forgotten.
84	T-PASS-222	Password Management	Can password changes be synchronized across multiple systems at the same time?	Fischer supports password synchronization as part of the solution. Fischer supports LDAP, Databases, Server Accounts, Google Apps, Office 365, among many others. Fischer has connectors for over 100 different applications; most of these connectors also provide password reset capabilities.
85	T-PASS-223	Password Management	Does the solution enforce password strength requirements?	Yes, requirement met out-of-the-box (OOB).

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
86	T-PASS-224	Password Management	Does the solution support the following password constraints: Minimum/maximum length, Minimum letters/numbers/special characters, Password history constraints, Exclusion dictionary, Allowable characters, Number of character types, Triviality checks (old password), ID in password check?	Fischer's password rules capability is unlimited. We will enforce any password policy required. We enforce password policy either at the system/synchronization group level or at the user level where different password policies may be enforced based on a user's membership in a security group, determined by attributes contained in their identity profile.
87	T-PASS-226	Password Management	Does the solution support multiple password policies per application? If Yes, can different policies be applied to users based on identity attributes (e.g., employee and contractor policies)?	Yes, requirement met out-of-the-box (OOB).
88	T-PASS-227	Password Management	Does the solution support challenge questions for password recovery?	Yes, requirement met out-of-the-box (OOB).
89	T-PASS-228	Password Management	Can the number of challenge questions presented to the user be configured based on the organization's security policies?	Yes, requirement met out-of-the-box (OOB).
90	T-PASS-230	Password Management	What verification methods (SMS text, email, etc.) are supported out of the box for self-service password reset or forgot password functions?	Fischer Identity supports email and text notification for password reset or forgot password functions.
91	T-PASS-231	Password Management	Can the solution support password intercepts, so as a change is made it can be quickly reflected across all managed systems	Requirement can only be partly met, customization is required to meet this requirement.
92	T-PC-187	Provisioning and Connectivity	Can the solution manage the complete user account lifecycle (add, edit and delete, enable, disable) for connected resources?	Yes, requirement met out-of-the-box (OOB).
93	T-PC-188	Provisioning and Connectivity	Can the solution validate that changes requested are correctly implemented in the target resource?	Yes, we can create a success task and do a look up in the target system to validate that changes requested are correctly implemented in the target resource.
94	T-PC-189	Provisioning and Connectivity	Does the solution provide a web-based interface for administration and configuration of application connectors?	Yes, requirement met out-of-the-box (OOB).

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
95	T-PC-191	Provisioning and Connectivity	Does the solution provide out-of-the-box connectors for the following categories of enterprise systems: LDAP directories, DB, Platforms (app servers), Business applications, Messaging applications, SaaS applications?	<p>Fischer provides out-of-the-box connectors for the following systems and applications for SaaS, hosted and traditional on-premise environments:</p> <p>Common/Core Systems</p> <ul style="list-style-type: none"> <li>• All systems and applications that support SPML v2</li> <li>• All systems and applications that support web services</li> <li>• All systems and applications authenticated by an LDAP server</li> <li>• All systems and applications authenticated by JDBC database</li> <li>• All systems and applications authenticated by Microsoft Active Directory</li> </ul> <p>Operating Systems / Authentication Systems including:</p> <ul style="list-style-type: none"> <li>o AIX</li> <li>o HP-UX</li> <li>o IBM 4690 Operating System</li> <li>o Linux</li> <li>o Microsoft Windows (2008, 2003, 2000) – (including deep folder permissions)</li> <li>o Microsoft Windows Command Line</li> <li>o MIT Kerberos</li> <li>o Novell NetWare – (including deep folder permissions)</li> <li>o RSA Authentication Manager</li> <li>o RSA SecurID</li> <li>o SCO UNIX</li> <li>o SQL Stored Procedures</li> <li>o Sun Solaris (with NIS, NIS+, directory authentication or</li> </ul>

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
96				<p>SSH)</p> <ul style="list-style-type: none"> <li>o UnixSSH</li> <li>o z/OS and OS/390 including subsystems: TSO, CICS, IMS-DC, etc. (RACF, ACF2 and Top Secret)</li> </ul> <p>Directories</p> <ul style="list-style-type: none"> <li>o Microsoft Active Directory (ADSI) - (including deep folder permissions)</li> <li>o Microsoft Active Directory Lightweight Directory Service (LDS) (formerly called ADAM)</li> <li>o Novell eDirectory</li> <li>o Novell Directory Service (NDS)</li> <li>o Sun Java System Directory Server, Sun ONE, iPlanet (now called Oracle Directory Server)</li> <li>o Oracle Internet Directory</li> <li>o IBM Tivoli Directory</li> <li>o CA Directory</li> <li>o Siemens DirX</li> <li>o 389 Directory (formerly called Fedora)</li> <li>o Red Hat Linux Directory</li> <li>o Open LDAP Directory</li> <li>o All other LDAP v3 directories</li> </ul> <p>Databases</p>

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
97				<ul style="list-style-type: none"> <li>o Oracle Database</li> <li>o MS-SQL Server</li> <li>o MS-Access</li> <li>o IBM DB2 Database</li> <li>o IBM Ingres Database</li> <li>o MySQL</li> <li>o Sybase Database</li> <li>o Informix Database</li> <li>o PostgreSQL Database</li> <li>o Progress Database</li> <li>o All other JDBC databases</li>   <li>Oracle E-Business Suite including:</li> <li>o Procurement</li> <li>o Contracts</li> <li>o Performance &amp; Daily BI</li> <li>o Customer Data</li> <li>o Customer Relationship</li> <li>o Financials</li> <li>o HR</li> <li>o Interaction Center</li> <li>o Learning</li> <li>o Logistics</li> <li>o Maintenance</li> <li>o Manufacturing</li> <li>o Marketing</li> <li>o Order</li> <li>o Product Lifecycle</li> <li>o Projects</li> </ul>

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
98				<ul style="list-style-type: none"> <li>o Sales</li> <li>o Service</li> <li>o Supply Chain</li> <li>o Transportation</li>   <li>Oracle-PeopleSoft – all applications including:               <ul style="list-style-type: none"> <li>o Asset Lifecycle</li> <li>o Campus Solutions</li> <li>o CRM</li> <li>o Enterprise Performance</li> <li>o Enterprise Service Automation</li> <li>o Financials</li> <li>o HCM</li> <li>o Supplier Relationship</li> <li>o Supply Chain</li> <li>o Enterprise Tools &amp; Technology</li> </ul> </li>   <li>SAP R/3 Enterprise and SAP NetWeaver (ABAP) applications including:               <ul style="list-style-type: none"> <li>o SAP Business Suite</li> <li>? SAP Customer Relationship Management</li> <li>? SAP ERP</li> <li>? SAP Product Lifecycle Management</li> <li>? SAP Supply Chain Management</li> <li>? SAP Supplier Relationship Management</li> <li>o SAP Human Capital Management</li> <li>o SAP Manufacturing</li> <li>o SAP Service and Asset Management</li> <li>o Alloy</li> </ul> </li> </ul>

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
99				<ul style="list-style-type: none"> <li>o Duet</li> <li>o Duet Enterprise</li> <li>o SAP BusinessObjects analytic solutions</li> <li>o SAP BusinessObjects business intelligence solutions</li> <li>o SAP BusinessObjects GRC solutions</li> <li>o SAP BusinessObjects EPM solutions</li> <li>o SAP Crystal solutions</li> <li>o SAP solutions for auto-ID and item serialization</li> <li>o SAP solutions for enterprise information management</li> <li>o SAP solutions for sustainability</li> <li>o Solution extensions</li>   <li>Help Desk / CRM / Service Center applications including:               <ul style="list-style-type: none"> <li>o Atlassian JIRA</li> <li>o Microsoft Dynamics CRM and IFD</li> <li>o SalesForce.Com</li> <li>• SSO and Federation including:                   <ul style="list-style-type: none"> <li>o Entrust GetAccess</li> <li>o Imprivata OneSign</li> <li>o RSA ClearTrust</li> <li>o Tivoli Access Manager</li> <li>o Tivoli Federated Identity Manager</li> </ul> </li> </ul> </li>   <li>Email including:               <ul style="list-style-type: none"> <li>o Microsoft Exchange</li> <li>o Lotus Domino / Notes (web client and Windows Client ID files)</li> </ul> </li> </ul>

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
100				<ul style="list-style-type: none"> <li>o Novell Groupwise</li> <li>o Fischer InterPost</li> <li>o Fischer TAO</li> <li>o IMAP servers</li> <li>o LDAP-compliant email systems</li> <li>o Microsoft Exchange Pagers</li> <li>o Zimbra</li> <li>o POP servers</li>   <li>Other applications including:</li> <li>o Accenture ITSM Remedy</li> <li>o AccPacc Pro</li> <li>o Blackberry Enterprise Server (BEIS)</li> <li>o Blackboard</li> <li>o Canvas LMS</li> <li>o Cerner Millennium Suite (approximately 50 healthcare applications)</li> <li>o Desire2Learn</li> <li>o Duo Security (two-factor authentication)</li> <li>o Google Applications</li> <li>o IBM 4690 Supermarket Application</li> <li>o Live@EDU</li> <li>o Luminis (through BEIS)</li> <li>o Microsoft Office365</li> <li>o Moodle</li> <li>o RCMS</li> <li>o SagePro (ERP)</li> <li>o Sakai</li> <li>o ServiceNow</li> </ul>



Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
101				<ul style="list-style-type: none"> <li>o Sungard Banner</li> <li>o WebEx</li> </ul> <p>Flat files including:</p> <ul style="list-style-type: none"> <li>o CSV</li> <li>o Excel</li> <li>o LDIF</li> <li>o Word</li> <li>o XML</li> </ul> <p>This list is continually growing as new integration methods are included in the product.</p>
102	T-PC-192	Provisioning and Connectivity	Does the application provide a solution for managing enterprise IT systems deployed in public or private clouds?	Yes, requirement met out-of-the-box (OOB).
103	T-PC-193	Provisioning and Connectivity	Does the solution provide users with detailed information about all provisioning tasks related to a request for access?	Yes, the user can view detailed information about any requests they have submitted.
104	T-PC-194	Provisioning and Connectivity	Describe how your solution recovers from failed fulfillment, transactions or provisioning attempts.	Fischer is capable of providing real time notification of such events, including remediation or "retry", in the event the failure was a result of target system unavailability. This includes the ability to log such events in the global log. Fischer provides further granularity from a logging perspective by enabling a distinct log per event type to be generated dynamically and hold data specific to the failed event and/or transaction. This empowers administrators to quickly identify and troubleshoot reasons why a particular event failed.

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
105	T-PC-196	Provisioning and Connectivity	Can the solution automate the revocation of permissions across applications? For example if permissions are adorned to an Active Directory group from another system does the system support the removal of permissions from a group?	<p>Fischer Identity's AD and OpenLDAP connectors include full functionality for group management within those directory structures. Group membership would be determined by qualifying for provisioning policies based on the user's identity attributes. Group and role membership can be determined based on any identity profile attribute.</p> <p>Fischer resource request process allows for internal names as well as external names and descriptions. In this case it is important that the display name/description gives good details to help the end user out. If they are still not able to figure it out, we have the ability to configure on behalf of (OBO) where other users have the ability to request for other users.</p> <p>Fischer Identity allows auditors, managers and service owners the ability to view access of users through the Self-Service and Admin UIs. A single user can be reviewed to see what access Fischer Identity shows the user is provisioned for.</p> <p>Fischer Identity has audit reporting for extracting data for analytical analysis for bulk reviews.</p> <p>Yes, you have the ability to develop additional directory synchronization on your own.</p>
106	T-PM-132	Policy Management	Does the system provide a business-friendly UI for defining and editing access policies without the need for coding?	Fischer provides a WYSIWYG approach for all interfaces which includes the ability to define and edit access policies without the need for coding.
107	T-PM-135	Policy Management	When policy violations are detected, does the application automatically notify responsible parties?	Yes, requirement met out-of-the-box (OOB).

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
108	T-PM-141	Policy Management	Are policy enforcement reports provided which outline users with active policy violations?	Fischer is able to log this information for our native application as it relates to authenticating to the interfaces, and tracking and detecting policy violations through various compliance and governance mechanisms. Compliance assessments can be executed on a scheduled basis to find (report) all access control policy violations and present audit controllers with remediation options as well as override options, including access certification.
109	T-R-037	Resilience	Please describe your Backup and recovery process. Attach or reference additional documents as necessary. Please include standard recovery time SLAs	Fischer Identity Supports this requirement. See Attachment F - Service Level Agreement.
110	T-R-038	Resilience	Please provide an overview of your disaster recovery plan (DRP) including measures such as offsite backup storage, RTO/RPO, warm/hot site availability.. Etc.	Fischer Identity is committed to 100% uptime for our federation / SSO environment. In the event of a disaster at our primary hosting facility, Fischer's disaster recovery platform will be available within 30 to 60 minutes of disaster detection/notification and confirmation. We are geographically dispersed. Fischer provides a hot spare data center with database replication of the production environment as well as archived database backups daily, kept for two weeks. 1 full backup is performed once per week with incremental backups every other day. For additional information, please see Attachment C - Data Breach Response.
111	T-RM-146	Role Management	Does the solution support custom types of roles?	Yes, requirement met out-of-the-box (OOB).
112	T-RM-147	Role Management	Can new role types be configured directly within the user interface?	Yes, requirement met out-of-the-box (OOB).
113	T-RM-148	Role Management	Can role engineers define additional metadata attributes on a role?	Yes, Fischer engineers can define additional metadata attributes on a role.
114	T-RM-152	Role Management	Does the solution support the ability to read or import organizational hierarchy information?	Yes, Fischer supports this requirement.
115	T-RM-153	Role Management	Does the solution provide a mechanism for combining business roles and IT roles into a common role model?	Yes, Fischer supports this requirement.
116	T-RM-156	Role Management	Does the solution support automated mining of both business roles (top-down) and IT roles (bottom-up)?	Fischer Identity currently does not have role mining services at this time. This is being explored.

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
117	T-RM-161	Role Management	Does the solution support role ownership? Does the solution support delegation with respect to role ownership?	Yes, the solution can support delegation with respect to role ownership. Customization is required to meet this requirement.
118	T-RM-166	Role Management	Does the solution support periodic role certification of both role composition (role privilege/entitlement mapping) and role membership?	Yes, requirement met out-of-the-box (OOB).
119	T-RM-168	Role Management	Can the solution detect and report on: inactive roles, users with no roles, and/or roles with no users?	Yes, requirement met out-of-the-box (OOB).
120	T-RM-171	Role Management	Can the solution provision changes for all users that have a particular role, when a role definition is changed?	Yes, Role based access can be configured per the business requirements of the Client. The client will need to provide the business rules and what access/resources each should get. Then this can be configured within Fischer using the configuration hub to set up your role-based solution. When a role changes, the solution will provision changes for all users that have that role.
121	T-RM-172	Role Management	Does the solution provide logging and reporting capabilities for all role changes? (e.g., "when was the role created, who created it, who approved it?")	Yes, requirement met out-of-the-box (OOB).
122	T-RM-174	Role Management	Does the solution support temporary assignment of a role to a user (e.g., sunrise and sunset dates)?	Yes, requirement met out-of-the-box (OOB).
123	T-RM-175	Role Management	Does the solution support the creation of temporary roles that have defined activation and deactivation dates?	Yes, Fischer has the ability to create temporary roles that have defined activation and deactivation dates.
124	T-RM-178	Role Management	Does the solution's role model enable users to have multiple accounts on a target system (e.g. standard and admin account) while providing automated role assignment and provisioning to the correct account?	Yes, requirement met out-of-the-box (OOB).
125	T-RSC-180	Risk Modeling	Does the solution support the assignment of unique risk values to each application, entitlement and role within the system?	No, Fischer does not support the assignment of risk values.

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
126	T-SR-007	Security Requirements	Do you have a 3rd party attestation of controls or certification such as an SSAE-16, ISO 2700X or a penetration test? Please provide any additional details that would demonstrate system controls.	<p>i. Dynamic vulnerability scanning is performed on a periodic basis. In depth knowledge of the IAM platform permits us to limit and filter false-positives.</p> <p>ii. Static analysis is performed as a part of Fischer's standard software development lifecycle.</p> <p>iii. Manual penetration testing is performed as determined by company management and is outsourced to a qualified third party.</p> <p>iv. Manual code review is performed as a part of Fischer's standard software development lifecycle.</p> <p>v. Threat modeling is performed annually by Fischer's internal security resources.</p> <p>vi. Security architecture review is performed annually by Fischer's internal security resources.</p> <p>vii. Malicious code analysis is outsourced to a qualified third party if and when it is discovered. To date, malicious code has never been detected within the Identity as a Service infrastructure.</p>
127	T-SR-009	Security Requirements	Please describe this system's Role Based Access Control capabilities, please include any Directory or SSO integration points and options.	This is standard functionality. Fischer can qualify / disqualify users with specific parts of their overall role(s). Grace periods can be assigned to remove distinct components of a role while leaving other parts untouched. This is all based on our ABAC / RBAC structure and within higher education is typically controlled by affiliations and roles.
128	T-SR-014	Security Requirements	Please list and explain all configurable or non-configurable password management controls including but not limited to: ( password complexity requirements, password expiration, password cycling, password recovery, system availability windows, password encryption, hashing and obfuscation, account lockout). Per Connector to system and/or by types of users	Fischer's password rules capability is unlimited. We will enforce any password policy required. We enforce password policy either at the system/synchronization group level or at the user level where different password policies may be enforced based on a user's membership in a security group, determined by attributes contained in their identity profile.

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
129	T-SR-015	Security Requirements	Please describe the systems Enterprise Single Sign-On (SSO) and Federated Identity capabilities. Please include Supported Technologies (i.e. SAML V2, OAUTH, etc.) as well as specific vendor integration partnerships and capabilities. Please note any known instances where your product DOES NOT integrative with SSO or Federated Identity Technologies or vendors.	Fischer provides an integrated Federated SSO IDP, based on Shibboleth, for those applications which are capable of accepting a SAML login. Fischer's approach to Federated SSO is somewhat different in having the IDP integrated with the IDM solution, allowing for tight control over the configuration and release of user attributes to downstream Service Providers and enhanced security through administrative credential management coming from encrypted credentials in the IDM system instead of preconfigured credentials in clear text in the IDP configuration files. Fischer's IDP will only release those user attributes to a downstream SP which have been configured in the SP definition. Those attributes are managed by and derived from the IDM system and the user's identity profile. Fischer Identity is an InCommon affiliate.
130	T-SR-016	Security Requirements	Please describe your system's native multi-factor authentication capabilities, please note any integration partners which are able to non-natively provide this capability	Fischer Identity supports provisioning and two-factor authentication using its own SMS and email based PIN verification, Duo Security, RSA SecurID and TOTP (time-based one time password). Other methods will be included and integrated as the technologies mature and as specific customer requirements dictate.

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
131	T-SR-017	Security Requirements	Please describe your system's provisioning and deprovisioning process. Please include any key technology employed and key integration partners which may be required.	Fischer Identity's provisioning engine allows for automated provisioning and de-provisioning across systems. Users qualify for policies (roles), these policies qualify a user for different access across different systems. Information from the source of authority will determine which policy/policies a user qualifies for. Fischer Identity includes connectors for many specialized systems and cloud services. In addition, Fischer's robust generic database, LDAP, and web services connectors allow for connectivity to many more systems that do not require the development of specialized connectors. If required, Fischer will develop up to three (3) connectors to commercially viable off-the-shelf applications at no additional cost, providing such new connectors are applicable to the majority of the Fischer customer base. Custom connectors for in-house applications can be developed for a fee.
132	T-SR-019	Security Requirements	What encryption technologies are employed by your system, and where are they employed?	Sensitive data at rest is encrypted. Where ever possible, sensitive data is stored using one-way hash. All communications are over secured channel. In transit data can also be encrypted for added security.
133	T-SR-020	Security Requirements	Please describe the capabilities to encrypt data at rest and in transit.	All communication between the user and the IDM solution is SSL encrypted, as is the communication between the Fischer Identity server and the Global Identity Gateway. Encryption at rest can be configured at the field level within the database for any sensitive data.
134	T-SR-021	Security Requirements	How often are external/third party penetration tests performed on the solution?	Quarterly, external/third party penetration tests are performed on the solution.
135	T-SR-022	Security Requirements	Which items of the solution are scanned as part of external / third party penetration tests?	Externally /third party penetrations tests are performed using QUALYS WAS. The items of the solution that are scanned include the Web Server, Certificates, and Database to identify vulnerabilities including cross-site scripting (XSS) and SQL injection.

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
136	T-SSO-234	SSO - Cloud/Web	Is an integrated Identity Provider (IdP) capability to provide password-free federated SSO via the SAML standard included with the solution, such as CAS or Shibboleth IdP?	<p>Fischer WebSSO solution is built on a Shibboleth IdP version 3.x stack and supports any protocols supported by the current IdP 3.x release.</p> <p>Fischer provides an integrated Federated SSO IDP, based on Shibboleth, for those applications which are capable of accepting a SAML login. Fischer's approach to Federated SSO is somewhat different, the IDP integrates with the IDM solution, this allows for tight control over the configuration and release of user attributes to downstream Service Providers and provides enhanced security through administrative credential management, coming from encrypted credentials in the IDM system instead of pre-configured credentials in clear text in the IDP configuration files. Fischer's IDP will only release those user attributes to a downstream SP which have been configured in the SP definition. Those attributes are managed by and derived from the IDM system and the user's identity profile. Fischer Identity is an InCommon affiliate.</p> <p>Fischer's IDP may be configured to front-end authentication to CAS and ADFS services for SSO integration of non-SAML targets, such as Microsoft products which rely heavily on ADFS for SSO functionality. In this way, all SSO functions can be incorporated into one user-facing solution.</p> <p>(continued in next row)</p>



Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
137	T-SSO-234 (continued)	SSO - Cloud/Web (continued)	Is an integrated Identity Provider (IdP) capability to provide password-free federated SSO via the SAML standard included with the solution, such as CAS or Shibboleth IdP? (continued)	<p>Fischer has developed a plugin for Active Directory which provides a seamless and true single sign-on experience for Windows desktop users. The SSO IDP can determine whether a user is connecting from behind the firewall or not. External users will be prompted for authentication by the IDP as expected. Connections from internal users trigger a query of the AD plugin as to whether the user has an active AD session through a Windows Gina login. If the user has already authenticated through a desktop logon, the IDP will not prompt the user for any further authentication unless required by policy, such as a second factor of authentication, providing a true clientless Single Sign-On capability.</p> <p>Fischer's self-service interfaces fully support SAML and CAS SSO login processes out of the box.</p> <p>Fischer provides users with a landing page experience for all of their SSO applications. This empowers the end users to click on the application they want to access without entering usernames and passwords.</p>
138	T-SSO-235	Enterprise Integrations	Should integrate with VCU's authentication / single sign-on (SSO) systems CAS or Shibboleth IdP via SAML 2.0. Alternatively, and less preferred, is integrating directly with Active Directory via LDAPv3 bind.	Fischer supports SAML 2.0 as the core of our SSO solution. Fischer can provide both IdP and SP services. Different systems have different mechanisms of SSO, and Fischer has integrated with multiple, some of which support http header-based authentication instead of SAML. Our LDAP authentication service fully supports LDAP version.
139	T-SSO-236	SSO - Cloud/Web	Does the solution deliver browser-based SSO functionality (i.e. federation, WAM)? Is it an additional module, or included with the solution?	Federation SSO is included as part of the full suite. it can be purchased as a separate module.

Fischer Response to VCU RFP For Identity and Access Management

	A	B	C	D
140	T-IT-071	Implementation and Training	How do you implement the product? If you work with external partners describe how you partner with these firms to implement your application.	Fischer has developed an implementation project methodology that ensures customer solutions are built on-time, within budget and to the customer's business and technical requirements. Fischer International Identity advocates and utilizes the agile project management methodology. As with any implementation, the X factor is the preparation, agreement and understanding of the requirements and solution specifications as well as ensuring the pre-requisites are met to install the product and ultimately build a solution. This process will take as long as is required, and the responsibility primarily lies with the customer pertaining to the defining and publishing the official solution requirements. It is important to note that our project timeline focuses on our ability to provide the required solution and not on the logistical hurdles that may occur. Our approach to projects drastically limits the liability associated with scope creep and validating prerequisites are met prior to engaging our technical team to actually perform the implementation. We've found this approach to streamline the solution construction phases. Please see Attachment A - Fischer Implementation Methodology.
141	T-IT-072	Implementation and Training	Please describe your training options for the technology solution. Please provide details such as computer-based, in-person, certifications, etc.	Fischer offers in-project solution transfer, as well as a 1 to 2 week onsite training course if required / desired by the customer. Training is dependent upon the selected deployment model. Cloud deployment typically provides remote train the trainer sessions for all end user facing interfaces. On-premise deployments will require the on-site training sessions. Customers are always welcome to come to our Naples, FL headquarters for training if desired. Costs for training are quoted in the initial services estimate.
142				

Fischer Response to VCU RFP For Identity and Access Management

Reference	Category	Question	Answer
PS-EXP-001	Experience and References	Describe your company's and years in business.	<p>Fischer is a pioneer and visionary in the identity management market and provided identity management technologies well before the market was named "identity management." During the 1990s, Fischer developed and marketed a metadirectory solution to meet our customers' requirement to synchronize data across disparate IT systems and directories. During that era, Fischer also developed and marketed password management capabilities and enabled user provisioning through scripting, as most vendors still do today. Fischer effectively had in the 1990s what many major vendors offer today: a suite of identity products composed of disparate technologies based on aged code bases.</p> <p>Fischer knew then that these early identity technologies would not be sufficient for managing identities and automating business processes in highly dynamic, heterogeneous IT environments: merging disparate identity technologies increases complexity and cost while decreasing reliability, programming business logic in workflows and policies is expensive and difficult to change, using "heavy" agent connectivity increases software costs and complicates deployments, and tracing identity activities across component-specific log databases adds time, cost and uncertainty to the audit process. In the early 2000s, Fischer shelved all of their existing identity solutions in favor of a designing and developing a solution that would truly simplify and reduce the cost of identity administration in diverse IT environments and easily extend to meet new business requirements.</p>

In 2005, Fischer set the stage for a new generation of identity management solutions that quickly enable new business processes and help customers manage more systems and resources with far greater ease, automation, and ROI than conventional approaches. Fischer's Global Identity Architecture® became the world's first holistic, standards-based identity management architecture with an ETL (extract, transformation, load) engine at its core, and eliminated the need for programming or scripting. Branded Fischer Identity™, organizations could choose from a suite of easily-configured identity modules and capabilities including provisioning, compliance, password management, privileged account management, self service and mobile password reset and provisioning approvals.

In 2007, Fischer extended its Global Identity Architecture® to offer identity management as a portfolio of secure and affordable outsourced services designed to fit any organization's needs. Fischer's Identity as a Service™ Solutions opened identity management benefits to the masses and created the Managed Identity Services® market by offering secure, right-sized identity services in Software-as-a-Service (SaaS) and hosted models.

Fischer International Identity has become a trusted Partner to Higher Education and provides extraordinary solutions that

have been awarded "Best Buy," "Market Leader," "Innovator of the Year," and other accolades. Fischer is a Visionary in the Gartner Magic Quadrant for user provisioning and the leader in Cloud-based Identity and Access Management (IAM). Being dedicated to the success of higher education institutions, Fischer is a member of Internet2, InCommon, and EDUCAUSE. The company is also a Platinum Sponsor of the PeopleSoft Higher Education User Group (HEUG) and is a member of the Vendor Council for the HEUG. Fischer also helps institutions join InCommon so they can take advantage of offerings from InCommon and Internet2 Net+ Services by helping them to meet the technical requirements of InCommon.

Today, Fischer has arguably become the most experienced and knowledgeable identity management vendor in the industry. Our customers are testimony to this fact. Most Fischer customers have previously owned a competitive identity product; they knew what they wanted and what to avoid. They chose Fischer.

Fischer was the first vendor to have its provisioning solution certified for use with PeopleSoft as this was prior to their acquisition by Oracle. Fischer is dedicated to the needs of higher education institutions with PeopleSoft and Fischer is on the Vendor Council for the PeopleSoft Higher Education User Group (HEUG) in addition to being a Platinum Sponsor of HEUG. To date, we have worked on PeopleSoft with two higher-ed institutions regarding PeopleSoft as well as a number of commercial customers.

Reputation: Fischer is respected worldwide as an authority in enterprise security. Our founder and chairman, Addison Fischer, is a founder of VeriSign, was the largest shareholder of RSA in its early years, has appeared by invitation before the United States Congress as an expert on software security-related matters, authored the now industry-standard mainframe security management product Top Secret (now sold and marketed by Computer Associates), and holds over 500 security-related patents.

Customer Base: Fischer International legacy products have been purchased by a significant percentage of Fortune 500 companies and Federal agencies. The Fischer Identity product customer base is currently over 3,000,000 users and is being used by over 5,000 companies across Higher Education, Finance, Healthcare, Manufacturing, Retail, and Government vertical industries, including the country's largest public university (95,000 enrollment).

Financial and Corporate Stability: Fischer is a privately-held corporation, and reflecting a longstanding policy, does not disclose financial information. However we consider our 30+ year history of financial stability and established customer base to be significant assets to our customers and partners. In lieu of financials, Fischer offers the following indicators:

Human Capital: 3 year employee base growth: 21% 3 year  
... .. 10% worldwide CEO

Fischer Response to VCU RFP For Identity and Access Management

			<p>employee base turnover: Less than 10% worldwide CEO tenure: Andrew Sroka joined Fischer in 1998 Approximately 67% of Fischer's workforce is devoted to software development and quality assurance Workforce (Dept): Research &amp; Development: 60% Sales/Marketing: 13% Customer Support &amp; Services: 24% Administrative: 3%</p> <p>Assurances: Escrow: Fischer will escrow source code for on-premise customers upon request with EscrowTech, a trusted, Fischer-selected intermediary. Surety Bond: Fischer is willing to secure a Surety Bond upon customer request Financial References: prospective customers and interested industry analysts are welcome to contact the references submitted under NDA.</p> <p>Please see Attachment H - Certificate of Insurance and Attachment I - Dunn &amp; Bradstreet report</p>
--	--	--	---

PS-EXP-002	Experience and References	Describe your company's background and history delivering identity and access management (IAM) integration services.	<p>Fischer has been delivering cloud-based IdM for more than 10 years, we understand the concerns of many colleges and universities with choosing a cloud-based IdM solution/service. While security is generally the largest concern, lock-in and ability to address future needs run close behind. Because we have a single IdM technology that can be deployed in a hosted environment or on-campus, Fischer customers always have the option to simply move the solution to either environment (and with guaranteed pricing). Regarding future capabilities and direction, our vision is to follow a user-focused approach that facilitates more efficient levels of secure access. We have introduced social login. We are introducing OpenID and OAuth enhancements, as well as additional multi-factor and mobile authentication mechanisms. We will continue to streamline our IdM delivery model so that IdM services can be more quickly rolled-out and consumed. As the focus of identity has shifted to authentication, authorization, analytics and risk-based framework and overall risk assessments as it relates to your solution and the VCU user population, Fischer is concentrating its development efforts to extend or add these capabilities.</p>
------------	---------------------------	--	--



PS-EXP-003	Experience and References	Describe your company's background and history delivering IAM integration services for this particular technology vendor including combined years of experience.	<p>FischerIdentity has many years of experience with clients in higher education. Each client is unique in their infrastructure, but most have similarities in their user population, business processes and roles required. This history gives us the ability to recommend best practices for implementing Identity Management.</p> <p>Our product methodology is likewise based on best practices. Our experience in deploying identity management solutions has resulted in a process that ensures we gather requirements, install components, complete the solution development and move to production in a very short turn around. This process also enables Fischer to guarantee implementation services fees and delivery date. See also response to 1.208: Warranty for Products and Services.</p> <p>Technology: History &amp; Innovations:          Fischer is recognized as a pioneer in the information security space and has been first-to-market with multiple solutions and technologies.          1980s: 1st PC Security Solution, 1st PC Security product rated by the National Security Center (NSC)          1990s: 1st Security Solution for Windows 95 and Windows NT. 1st meta directory on IBM z/OS          2000s: 1st SOA-compliant Identity Management Architecture, 1st Provisioning Solution Validated for Oracle / PeopleSoft, 1st Mobile Password Reset and Provisioning Approval Solution, 1st IAM solution to eliminate scripting and programming requirements</p>
------------	---------------------------	--	---

Fischer Response to VCU RFP For Identity and Access Management

			<p>2010s: 1st Identity Management Solution for SaaS/Cloud delivery</p> <p>Technology: Recognition:                  2015, 2014, 2013: Gartner Identity Governance and Administration (IGA) Magic Quadrant                  2015, 2014, 2013, 2012: Gartner Identity as a Service (IDaaS) Magic Quadrant / Market Studies                  2013: "Champion: IAM Services." Bloor Research                  2013: "Product Leader" KuppingerCole Access Governance Leadership Compass                  2012, 2011, 2010, 2009, 2008, 2007: Gartner User Provisioning Magic Quadrant: Visionary Quadrant                  2012, 2011, 2010: "Best Buy: Identity Management." Secure Computing Magazine</p>
PS-EXP-004	Experience and References	Describe your company's status as an authorized reseller, or authorized partner of the technology vendor.	Fischer develops and maintains the Fischer Identity software. No part of the development is outsourced to any third party entities.

PS-EXP-005	Experience and References	What differentiates your company from its competitors for implementation services?	<p>Culture - The biggest difference between us and our competition is our Culture; it drives every decision we make. We're customer advocates and propeller heads, meaning that we listen to our customers and are very good at creating solutions that meet customer needs. And that's very apparent in our solutions; we've taken a completely different approach to managing the Identity Lifecycle so customers are able to secure more parts of the campus with less effort and cost, start benefiting from the solution in weeks vs. years, minimize or eliminate professional services, and quickly respond to changes. Our company has been structured to ensure that we strive to meet customer expectations every day: deployment times, technical support, licensing, product roadmap, etc.</p> <p>Higher education specialization -We understand higher education processes, systems/technical environments, users, business challenges, goals, and missions.</p> <p>Choice of Deployment Model - We offer both on-site software or hosted cloud subscription</p> <p>Ease and Speed - Ability to easily and quickly change and extend the solution to meet new business requirements.</p> <p>Experience - Fischer has 30-year history in information security and has been developing identity management solutions since before the sector was called "identity management."</p>
------------	---------------------------	--	---

PS-EXP-005	Experience and References	<p>What differentiates your company from its competitors for implementation services? (continued)</p>	<p>(continued)                      Full-time equivalent student license model - License fee is based on FTES enrollment count, yet provides licenses for 10-times that number so that institutions can service more user populations without adding cost.</p> <p>Guaranteed Implementation Time and Cost - Deployment cost is locked BEFORE the solution is purchased; Fischer will pay the customer a penalty fee for every day the project is late* (terms apply).</p> <p>Minimal Professional Services - Ease of implementation minimizes costs.</p> <p>Time to value - Fischer is setting unprecedented deployment times as a result of "configuration vs. customization" approach, Agile project methodology, and strong project management.</p> <p>Reference:  <a href="http://campustechnology.com/articles/2014/09/24/mi...">http://campustechnology.com/articles/2014/09/24/mi...</a></p>
------------	---------------------------	---	---

PS-EXP-006	Experience and References	Describe your track record, and give examples and previous performance delivering similar integration services.	<p>CONFIDENTIAL: Over 60% of all Fischer customers are higher education institutions. We understand the business processes, systems, user communities, needs and challenges that are unique to the Higher Education Enterprise - and our solutions and deployment methodology show it. Since launching Fischer Identity in 2005, 98% of all identity management deployments have been delivered successfully, and we are proud to have a 97% customer retention rate within higher education. We are constantly innovating and evolving our product and fine-tuning our methodology. We are never satisfied because we know we can continue to make IAM easier. We have evolved IAM deployment efficiency and predictability to the point where our 2016 IAM projects are going-live within 8 to 12 weeks after the Statement of Work is approved, and without any changes to scope or budget. Two such deployments are detailed below to illustrate project scope and university business processes.</p> <table border="1" data-bbox="1325 781 1913 1360"> <thead> <tr> <th></th> <th>Private Not-for-Profit University</th> <th>Private Not-for-Profit University</th> </tr> </thead> <tbody> <tr> <td><b>Model</b></td> <td>On Premise</td> <td>IaaS® Cloud</td> </tr> <tr> <td><b>Users</b></td> <td>6,000 Students, Faculty, Staff</td> <td>15,000 FTES plus Faculty, Staff, Contractors, Guests</td> </tr> <tr> <td><b>Business Activities</b></td> <td>Automated <u>Automated</u> Identity Life Cycle Management for Students and Employees, (including combinations of multiple affiliations) across core university business processes, e.g., Student (admissions, registration, graduation, etc.); Employee (onboarding, ongoing change, <u>offboarding</u>); Guests (onboarding, offboarding)</td> <td>Automated <u>Automated</u> Identity Life Cycle Management for Admits, Students, Employees, Contractors, Retirees, and Guests (including combinations of multiple affiliations) across core university business processes, e.g., Student (admissions, registration, graduation, etc.); Employee (onboarding, ongoing change, <u>offboarding</u>); Guests (onboarding, <u>offboarding</u>)</td> </tr> <tr> <td><b>Capabilities</b></td> <td>Full Suite IAM + SSO</td> <td>Full Suite</td> </tr> <tr> <td><b>SoA</b></td> <td>Banner</td> <td>Banner</td> </tr> <tr> <td><b>Target Systems</b></td> <td>Banner, PeopleSoft, AD, Oracle DB, O365, Box, Oracle Direct Access</td> <td>AD, PeopleSoft, Google Apps, Oracle DB, LDAP, Shares, Card System</td> </tr> <tr> <td><b>Workflows</b></td> <td>70</td> <td>43</td> </tr> <tr> <td><b>Access Policies</b></td> <td>10</td> <td>20</td> </tr> <tr> <td><b>Time to Value</b></td> <td>8 Weeks</td> <td>12 Weeks</td> </tr> </tbody> </table>		Private Not-for-Profit University	Private Not-for-Profit University	<b>Model</b>	On Premise	IaaS® Cloud	<b>Users</b>	6,000 Students, Faculty, Staff	15,000 FTES plus Faculty, Staff, Contractors, Guests	<b>Business Activities</b>	Automated <u>Automated</u> Identity Life Cycle Management for Students and Employees, (including combinations of multiple affiliations) across core university business processes, e.g., Student (admissions, registration, graduation, etc.); Employee (onboarding, ongoing change, <u>offboarding</u> ); Guests (onboarding, offboarding)	Automated <u>Automated</u> Identity Life Cycle Management for Admits, Students, Employees, Contractors, Retirees, and Guests (including combinations of multiple affiliations) across core university business processes, e.g., Student (admissions, registration, graduation, etc.); Employee (onboarding, ongoing change, <u>offboarding</u> ); Guests (onboarding, <u>offboarding</u> )	<b>Capabilities</b>	Full Suite IAM + SSO	Full Suite	<b>SoA</b>	Banner	Banner	<b>Target Systems</b>	Banner, PeopleSoft, AD, Oracle DB, O365, Box, Oracle Direct Access	AD, PeopleSoft, Google Apps, Oracle DB, LDAP, Shares, Card System	<b>Workflows</b>	70	43	<b>Access Policies</b>	10	20	<b>Time to Value</b>	8 Weeks	12 Weeks
	Private Not-for-Profit University	Private Not-for-Profit University																															
<b>Model</b>	On Premise	IaaS® Cloud																															
<b>Users</b>	6,000 Students, Faculty, Staff	15,000 FTES plus Faculty, Staff, Contractors, Guests																															
<b>Business Activities</b>	Automated <u>Automated</u> Identity Life Cycle Management for Students and Employees, (including combinations of multiple affiliations) across core university business processes, e.g., Student (admissions, registration, graduation, etc.); Employee (onboarding, ongoing change, <u>offboarding</u> ); Guests (onboarding, offboarding)	Automated <u>Automated</u> Identity Life Cycle Management for Admits, Students, Employees, Contractors, Retirees, and Guests (including combinations of multiple affiliations) across core university business processes, e.g., Student (admissions, registration, graduation, etc.); Employee (onboarding, ongoing change, <u>offboarding</u> ); Guests (onboarding, <u>offboarding</u> )																															
<b>Capabilities</b>	Full Suite IAM + SSO	Full Suite																															
<b>SoA</b>	Banner	Banner																															
<b>Target Systems</b>	Banner, PeopleSoft, AD, Oracle DB, O365, Box, Oracle Direct Access	AD, PeopleSoft, Google Apps, Oracle DB, LDAP, Shares, Card System																															
<b>Workflows</b>	70	43																															
<b>Access Policies</b>	10	20																															
<b>Time to Value</b>	8 Weeks	12 Weeks																															

Fischer Response to VCU RFP For Identity and Access Management

PS-APP-007	Experience and References	Please provide five (5) reference accounts where you implemented this particular technology solution. Two (2) of these references should include user / identity populations over eight-thousand five hundred (8500). Please indicate which references are higher education if any.	Please see Attachment G - References for RFP
PS-APP-008	Approach	Describe your recommended approach including project activities, project management, dependencies, assumptions, deliverables, milestones, success criteria and phases. Please include any samples or templates.	Fischer has developed an implementation project methodology that ensures customer solutions are built on-time, within budget and to the customer's business and technical requirements. Fischer International Identity advocates and utilizes the agile project management methodology. As with any implementation, the X factor is the preparation, agreement and understanding of the requirements and solution specifications as well as ensuring the pre-requisites are met to install the product and ultimately build a solution. This process will take as long as is required, and the responsibility primarily lies with the customer pertaining to the defining and publishing the official solution requirements. It is important to note that our project timeline focuses on our ability to provide the required solution and not on the logistical hurdles that may occur. Our approach to projects drastically limits the liability associated with scope creep and validating prerequisites are met prior to engaging our technical team to actually perform the implementation. We've found this approach to streamline the solution construction phases. The table below outlines the phases that encompass our implementation approach. Please see Attachment A - Fischer Implimentation Methodology.

PS-APP-009	Approach	<p>Please provide a proposed staffing and resource plan including type of staff member, skillset-level of staff member, hours or percentage of time dedicated, and other details you expect is required to deliver the required scope.</p>	<p>Each project will include a Fischer Project Manager, Technical Lead, and Implementation lead to plan and build out the design of your solution per your requirements. The Project Manager and Technical Lead will remain connected through the lifecycle of the project. Once the preliminary design of the solution and the project hours are agreed to by Fischer and the client, Fischer assembles a team of Implementation Engineers to perform the work outlined in the Statement of Work. The number of Implementation Engineers that are assigned to the implementation phase of the project is based on the complexity of the work to be performed, as well as the amount of hours involved in the implementation phase.</p> <p>Project Manager - Responsible for all logistics related to the execution of the project. Responsibilities include ensuring project deadlines and milestones are met, risk identification, planning, defining scope.</p> <p>Technical Lead - Responsible for identifying and gathering all technical requirements related to the project. Responsibilities include working with the Implementation Lead and Project Manager to create the Statement of Work, Preliminary Design Specifications, and the architecture of the solution based on the client requirements.</p> <p>Implementation Lead - The Implementation Lead that is assigned to the project is engaged with the Technical Lead throughout the project to build out the solution based on the client requirements. During the implementation phase, the Implementation Lead is engaged in the construction of the solution and also serves as the solution subject matter expert to ensure that the solution is constructed based on the requirements agreed to by the client and Fischer.</p>
------------	----------	--	---

Fischer Response to VCU RFP For Identity and Access Management

PS-REQ-010	Approach	Provide a list of VCU personnel required to support the proposed activities, including estimated number of hours required, specific skillsets and expertise.	Network Administrators - Initial configuration of the network to ensure secure communications to the Fischer Identity Suite. This is a onetime setup for both Production and Development environments. 1 week, 20% of their time. Server Administrators - Standing up of servers required for the solution. 2 weeks, 25% of their time. Project Manager - Responsible for keeping project on task on the Cal State side. On going, 10% of their time. Application Owners - Responsible for providing details on the application so our team can perform the solution construction. Also involved in testing of the solution when completed. On going, 15% of their time. Time is dependent on the complexity of the target systems.
PS-INFA-011	Requirements Documentation	Must jointly document business requirements, functional requirements, and non-functional requirements to support this solution and its implementation.	In addition to the Self-Service documentation and online help. Fischer will provide a written solution debrief to help the customer.
PS-INFA-012	Infrastructure Requirements	Provide consultative advice to VCU regarding infrastructure requirements, planning and architecture so that the minimum infrastructure meets the solution's needs.	Please see Attachment B- Official Project Pre-requisites Guide for the resources and infrastructure requirements.
PS-INST-013	Infrastructure Requirements	Irrespective of on-premise or cloud-hosted, describe the minimum infrastructure required to support the technology solution, and implementation services. Include numbers, specifications and details for servers, operating systems, databases, network dependencies (i.e. NLB), TLS/SSL certifications, and storage. Please include additional licensing costs if required. This will be for two non-production (i.e. development and QA), and one production environment.	Fischer Identity requires the customer install a Global Identity Gateway (GIG) to enable security communication between the cloud and the customers network. The GIG may be installed in a clustered mode. Separate GIG instances will be needed for production and test environments. Each data center hosting systems being managed by Fischer will need to have a GIG or GIG Cluster installed in it.



Fischer Response to VCU RFP For Identity and Access Management

PS-INST-014	Installation Requirements	Must install and configure technology solution in two non-prod (i.e. development and QA), and one production environment.	Fischer advocates a test environment that is separate from production. This is our standard operating model for solution building. Fischer does not charge extra for test and development instances of the product. Customers may install as many instances of Fischer Identity as they need to accomplish their mission goals. Configurations developed in a test environment may be exported from test and imported into production with only hostname/IP address and system account changes required to complete the move.
PS-INTEG-015	Installation Requirements	Must jointly integrate technology solution with VCU's infrastructure ecosystem to provide backups and disaster recovery, and to be made accessible within VCU's network.	Fischer provides a hot spare data center with database replication of the production environment as well as archived database backups daily, kept for two weeks. 1 full backup is performed once per week with incremental every other day. For additional information, please see Attachment C - Data Breach Response.
PS-INTEG-016	Enterprise Integrations	Should integrate with the enterprise mail system, to send email-based notifications for information and approval purposes.	Fischer Identity supports notification for requests, approvals, and access expiration. Fischer provides a notification queue feature that shows the status of all notifications sent through the system, including who it was sent to, the success or failure of the message as well as the content of the message.
PS-INTEG-017	Enterprise Integrations	Provide integration with VCU's IBM QRadar system for syslog events.	Fischer Identity uses log4J and that can log to any log server that is listening. In addition, other components used like Apache Tomcat, Apache HTTP server or Microsoft IIS server already have in-built capabilities to integrate with SIEM tools. If the SIEM tool is not capable of doing direct integration, then log files can be shipped to SIEM tools automatically.
PS-INTEG-018	Enterprise Integrations	Should integrate with VCU's authentication / single sign-on (SSO) systems CAS or Shibboleth IdP via SAML 2.0. Alternatively, and less preferred, is integrating directly with Active Directory via LDAPv3 bind.	Fischer supports SAML 2.0 as the core of our SSO solution. Fischer can provide both IdP and SP services. Different systems have different mechanisms of SSO, and Fischer has integrated with multiple, some of which support http header-based authentication instead of SAML. In some cases, development work is required.

Fischer Response to VCU RFP For Identity and Access Management

PS-LCM-019	Enterprise Integrations	Should provide consultative advice to VCU for configuration of application-layer and middleware layer monitoring as required.	Fischer IaaS Infrastructure team who maintain the IAM SaaS platform can provide consultative advice to VCU for design, implement, configure and administer IAM solution. In addition, they can provide guidance in selecting and implementing monitoring and alerting solutions and best practices.
PS-LCM-020	Identity Lifecycle Requirements	Should integrate with VCU's on-premise system of record (SOR) authoritative source of identity information, Banner, ideally through its Banner Enterprise Identity Services (BEIS) for near real-time identity updates.	Fischer Identity supports this requirement. Fischer supports receiving Banner BEIS SPML messages for real time transactional based provisioning.
PS-LCM-021	Identity Lifecycle Requirements	Must be able to identify primary types of users (students, faculty, staff, affiliates, etc.) and provision access based on this information. These primary types (i.e. enterprise roles, business roles, etc.) of users are not mutually exclusive, as a user can be a staff member and student at the same time.	Fischer Identity supports this requirement.
PS-PROV-022	Identity Lifecycle Requirements	Must be able to uniquely identify the user authoritative source systems and VCU-managed algorithm to generate unique identifiers and email addresses.	Fischer Identity supports this requirement.
PS-PROV-023	User Provisioning Requirements	Must be able to identify events used to trigger provisioning and access events, including joiner (i.e. hire, new student), mover (i.e. transfers) and leaver (i.e. terminate, former student).	Fischer Identity can automatically add/change/revoke user access to IT and physical assets based on real-time events (e.g., matriculation, new hire, furlough) and self-service requests all in compliance with your policies.
PS-PROV-024	User Provisioning Requirements	Automatically provision (e.g. "birthright provisioning") for key systems based on application-specific roles outlined in section XXXX.	Fischer Identity supports this requirement.
PS-PROV-025	User Provisioning Requirements	Automatically deprovision key systems outlined in section XXXX.	Fischer Identity supports this requirement.

Fischer Response to VCU RFP For Identity and Access Management

PS-PASS-026	User Provisioning Requirements	Provide a method to "Emergency Terminate" and immediately disable access where authoritative "leaver" or "term" data is not received in a timely manner.	Fischer provides multiple methods to accomplish this use case. The typical process is via the authoritative source where key information changes and the user's account is recognized as terminated. At this point Fischer's RBAC / ABAC engine will disqualify the user and de-provision (delete or disable). In cases where more immediate action is required, administrators can forcibly disable all access for a user immediately, in affect freezing all accounts until further notice.
PS-PASS-027	Password Management Requirements	Should replicate passwords changes from IAM solution to NetIQ eDirectory and Active Directory.	Fischer supports updating Active Directory passwords. Fischer can support password management into any target system that allows for that integration. Fischer has a collection of "connectors" that allow for this functionality out of the box. If a target system is not currently in the Fischer Connector library, one can be added. Fischer utilizes the agile project methodology which allows for creation, testing and deployment of connectors in a short timeframe.
PS-PASS-028	Password Management Requirements	Must provide an end-user facing self-service password reset (SSPR) interface so that users can regain access to their account if they forgot their password, or are otherwise locked out of their account.	Fischer provides self-service mechanisms enabling end users to reset passwords via the legacy question / answer approach as well as BYOD method's empowering end users to receive a PIN to their smart phone or SMS enabled device that can be used to verify identity
PS-RPRT-029	Password Management Requirements	Must provide custom email-based reminder notifications for passwords that will be expiring, with instructions on how to change and manage their password.	Password Expiry Notifications can be configured to meet this requirement.
PS-RPRT-030	Reporting Requirements	Should configure and validate reports for account (type, state and status), orphan accounts, idle accounts, excessive access (against roles, rules and policy) for each integrated application outlined in Section XXXX.	Fischer provides mechanisms to detect the existence of orphan accounts, idle accounts, excessive access for integrated applications. This information is presentable in a report format to the customer so that the customer is able to remediate those actions accordingly.
PS-RPRT-031	Reporting Requirements	Should configure and validate reports for password management events: forgot password, unlock password, reset password, etc.	Fischer Identity meets this requirement.

Fischer Response to VCU RFP For Identity and Access Management

PS-TEST-032	Reporting Requirements	Should configure and validate reports for # of provisioned, deprovisioned, etc.	<p>Fischer provides an accessible audit store that contains information about all actions and activities that occur within the platform. Fischer is able to log this information for our native application as it relates to authenticating to the interfaces, and tracking and detecting policy violations through various compliance and governance mechanisms. Compliance assessments can be executed on a scheduled basis to find (report) all access control policy violations and present audit controllers with remediation options as well as override options, including access certification.</p> <p>The audit store is a well-organized database that is queried from Fischer's native reporting interface, or externally from third party reporting tools like Crystal (or direct DB queries). There are approximately 100 out-of-the-box reports available plus the ability to create custom reports covering all aspects of the platform in a multitude of views. Reports can also be scheduled to run periodically and notify concerned auditors when complete. Auditors can login into self-service portal to view the reports.</p>
PS-TEST-033	Testing Requirements	Must document and deliver test plan and test cases that appropriately validate business, functional and non-functional requirements.	<p>Unit testing and Integration of the solution will be done by the implementation team during the implementation sprint. After a successful run through of all requirements, the solution will be given to the customer to do full acceptance testing including various scenarios of functionalities and business logic as well as stress/volume testing along with all required tuning at various iterations. After successful completion of multiple iterations of tests, the solution can be moved to production. A sanity test will be done in production to ensure everything is working as required.</p>
PS-TEST-034	Testing Requirements	Must validate requirements through functional testing and system-integration testing in a non-production environment.	Fischer provides a test environment

Fischer Response to VCU RFP For Identity and Access Management

PS-TRN-035	Testing Requirements	Should jointly perform user acceptance testing in coordination with VCU.	Once the Fischer Implementation team has completed the Solution Construction phase, the solution is turned over to the customer to perform user acceptance testing. During the UAT phase, any issues that arise can be submitted to Fischer in the form of a ticket by the customer, this allows for a single communication channel and eliminates the need to manage spreadsheets and multiple documents for issue tracking. Reported issues are quickly re-mediated. Historically, customers typically require 30-45 days for user acceptance testing.
PS-TRN-036	Training	Must provide documented installation and configuration, end-user, administrative and support guides.	Fischer provides an extensive amount of documentation covering every aspect of the product.
PS-DEPL-037	Training	Must provide training to VCU's IAM team regarding the customizations and configurations in support of the custom requirements.	Onsite training is included as a part of the initial project; training includes in-project solution transfer as well as a 1 to 2 week onsite training course. Solution training covers core components of the Fischer self-service user interfaces, including walkthroughs of the Admin/OBO functionality and how end-users will interact with self-service based on your requirements.
PS-DEPL-038	Deployment Requirements	Should perform and provide reports regarding system performance, load and capacity measurements prior to go-live.	Fischer will provide reports regarding system performance, load and capacity measurements prior to go-live. Performance metrics reports are available upon request. The IaaS Infrastructure team monitors application and database performance using various tools like Nagios, JMC and native tools available with various components used in production. In addition, Fischer's in-built monitor dashboard shows real time performance.
PS-DEPL-039	Deployment Requirements	Must provide implementation procedures that describe the activities required to deploy or promote the configurations and customizations into a higher-level environment (i.e. non-production to production), including a roll-back plan, and criteria used to confirm successful deployment (i.e. implementation checklist).	We work directly with the customer to deploy solutions into the production environment after completion of UAT. The process includes user and solution migration from the test environment into the production environment. We will provide training and documentation that describe the activities required to deploy or promote the configurations and customizations into a higher-level environment (i.e. non-production to production), including a roll-back plan, and criteria used to confirm successful deployment (i.e. implementation checklist).

Fischer Response to VCU RFP For Identity and Access Management

<p>PS-DEPL-040</p>	<p>Deployment Requirements</p>	<p>Must provide consultative support for implementation activities, and up to 2 weeks of post go-live support.</p>	<p>Fischer provides the customer with full support during the production migration and go-live including, but not limited to; preparing and testing necessary workflow processes to perform user loads into Fischer, working with the necessary members of the customer's project team to assist with any connectivity issues to connected systems. Fischer technical leads assigned to the project remain engaged for 30 days after solution go-live to assist with and re-mediate any issues that may arise. After the 30 day post-production support period, the solution is transitioned to our Solution Management team for continuous support. Prior to solution turnover to the Solution Management team, the Fischer technical lead assigned to the project will present the design and functionality of the solution to the team. This engagement ensures that the Solution Management team understands and is prepared to provide you with an exceptional support experience to assist with any of your support needs.</p>
--------------------	--------------------------------	--	--

Reference	Category	Question	Answer
C-SLC-001	Software Licensing Costs	Briefly describe your solution's pricing structure, terms and conditions, including licensing model (per user, site, enterprise, systems, CPU, tiers, subscription, concurrent users, etc.), delivery methods (SaaS, on-premise, etc.), and maintenance pricing for each.	See Attachment E - Pricing Methodology.
C-SLC-002	Software Licensing Costs	Do you provide pricing models specific to Higher Learning institutions?	Student FTE pricing was designed with the assistance of colleges and universities to create a clear, predictable, and easy-to-administer license model that is based solely on the institution's Student FTE enrollment. It provides the benefits of an "enterprise license" but at significantly-reduced cost. License fees are based only on the FTE Student enrollment; there are no license fees for Authorized Non-FTES users (e.g., faculty, staff, alumni, applicants, guests, parents, etc.). The Authorized Non-FTES User population is set at 10-times the Student FTE count. Inactive users do not consume licenses (e.g., users that are stored in the Fischer system for archival purposes) There are no license or maintenance fees for connectors (excluding connectors for custom or non-commercially viable systems). Fischer does not require True-up until actual Student FTE exceeds licensed FTE by 5%.
C-SLC-003	Software Licensing Costs	Are there additional costs involved in maintaining non-production environments, disaster recover (DR) environments in production? Please provide estimates.	All costs are reflected in provided pricing.
C-SLC-004	Software Licensing Costs	What are the costs associated to subcomponents of the systems, including connectors, connector kits, adapters and other tools?	There are no additional costs for subcomponents or connectors.
C-SMC-001	Software Maintenance Costs	What are the annual maintenance costs for using the system? How is maintenance calculated year over year, from one year to the next? Is there a cap on maintenance increase each year at a maximum that is consistent with the Special Terms and Conditions of the RFP?	Annual Software Maintenance is calculated at 22% of initial licensing fees for on premise deployments. There are no maintenance increases during the initial term of the agreement. Upon subsequent renewal Fischer International may, with prior written notice to the client, increase annual software maintenance and such increase shall not be greater than the greater of (i) the annual percentage increase in the Consumer Price Index published by the United States Department of Labor, Bureau of Labor Statistics, in effect at the time, from the prior year, or(ii) three percent (3%)..
C-SMC-002	Software Maintenance Costs	Describe what's included in maintenance. Are future versions included in maintenance, or are net-new licenses required for future major releases?	All in-version updates, patches, hot fixes, and component upgrades are included in maintenance. Major Releases (version changes) may require additional professional services, however there are no licensing fees associated with any upgrades.
C-SMC-003	Software Maintenance Costs	Are there cost associated with providing technical support? If yes, describe for support during the business day and on	Technical Support is included with maintenance for on-premise deployments, and within the annual service fees for hosted solutions. Service Support and
C-SMC-004	Software Maintenance Costs	Describe what's included in support. Are there additional costs/charges for esclations or customer-success management? What	There are no additional costs for escalations or solution management.
C-SMC-005	Software Maintenance Costs	Please list any other costs that a client with a similar higher-education profile, similar to VCU may have to incur to use the solution.	There are no additional costs associated with the solution. For on-premise deployments, Fischer International does not provide any hardware or
C-ICD-001	Implementation Costs and Details	What are the standard rates for your business analysts?	Our standard costs for Higher Education Professional Services resources are \$175/hour
C-ICD-002	Implementation Costs and Details	What are the standard rates for your technical architects, consultants and developers?	Our standard costs for Higher Education Professional Services resources are \$175/hour
C-ICD-003	Implementation Costs and Details	What are the standard rates for your project managers?	Our standard costs for Higher Education Professional Services resources are \$175/hour

C-ICD-004	Implementation Costs and Details	Please describe your recommended deliverables with the solution implementation, including any remaining toolkits, tools or work product resulting. What are your expectation around ownership of intellectual property or use of the work products or deliverables?	<p>Staffing Assumptions</p> <p>Network Administrators - Initial configuration of the network to ensure secure communications to the Fischer Identity Suite. This is a onetime setup for both Production and Development environments. 1 week, 15% of their time.</p> <p>Server Administrators - Standing up of servers required for the solution. 1 weeks, 25% of their time.</p> <p>Project Manager - Responsible for keeping project on task on the Cal State side. On going, 10% of their time.</p> <p>Application Owners - Responsible for providing details on the application so our team can perform the solution construction. Also involved in testing of the solution when completed. On going, 10% of their time. As a part of the initial project, Fischer builds training hours into the original services cost estimate. This includes in-project solution transfer as well as a 1 to 2 week onsite training course.</p> <p>Ownership of intellectual property is listed in the contract.</p>
C-ICD-005	Implementation Costs and Details	Please describe your recommended approach to implementing the solution.	Please see Attachment A Fischer Implementation Methodolgy.
C-ICD-006	Implementation Costs and Details	Please describe your expected assumptions and dependencies from VCU in implementing the solution? What are the risks associated with these assumptions and dependencies.	<p>Staffing Dependencies and Assumptions: Throughout the life cycle project, Fischer works closely with the appropriate customer technical and business staff assigned to the project. The customer engagement during the implementation is paramount to the overall success of the project. Without full customer engagement throughout the project, risks such as project slippage and scope creep can occur. The below list provides an overview of the staff roles and the expected level of engagement that are necessary to ensure a successful implementation.</p> <p>CIO, Director or authorized representatives – Staffing qualified to discuss and make definitive decisions related to business process and overarching security, identity and access management policies. Participants at this level are crucial to ensure the project is sponsored appropriately. This is to ensure when automation is introduced there is a proper level of expectation and authorization as to how it will work and scope creep is kept to minimum. These participants are needed to kick off the project and to set the proper tone and level of expectation for the internal staff. Escalations will occur from time to time related to specific business decisions that are required before a configuration can be completed. Participants from this group should be connected to the project from beginning to end, with heavy participation in the early stages and user acceptance testing phases.</p> <p>Infrastructure Management / Network Administration – Staffing qualified to discuss and make definitive decisions related to the infrastructure and architectural layer of the solution are required in the early stages of the project. The solution requires access to web services channels in order to properly communicate with application components as well as throughout the customer's network. Often times this requires firewall modifications, DNS changes and public SSL certificate signing configurations and procedures. Decisions are also needed and resource allocation is required to standup servers (virtual or physical) and install operating systems. OS software. These participants</p>



physical) and install operating systems, OS software, etc. These participants are typically needed in the early stages of the project and the need for their time fades as the project progresses. These participants ensure the platform is up and running, the software is able to be installed and communicate with the requirement components and all components are able to successfully communicate in a secure manner.

Application Analysts / Application Owners – Application-layer participants are critical to the success of the project. Participants from this group hold crucial information required for a successful deployment. Downstream target application provisioning and password management requirements are the most important component to a success full-suite IAM deployment. Application owners must be intimately involved in the project from beginning to end. Target system-specific knowledge will be critical as automated processes are built and the associated business workflows are defined. Application owners and analysts are almost always the ones able to say if the configuration is right or wrong; and if the configuration is wrong, they are able to explain exactly what is not correct and how Fischer should correct it. Participants from this group should never disconnect from the IAM solution as they are the persons most affected by the solution and they must stay aware and engaged at all times. The skillsets required including the ability to think logically through business policy and business rules and apply that logic in a scripting format. There is no specific language required however understanding scripting methodology and syntax is a critical qualification. This skill is typically found in the application owners, with specific knowledge of how their system(s) work.

Database Administrators – DBAs play a crucial role to the success of the solution. Fischer's application is a database-drive application, therefore customer DBAs must be intimately involved in the initial infrastructure setup phases to ensure the proper permissions and schemas are accessible. Subsequent phases require the DBAs presence to ensure clustering and other database optimizations are configured to ensure the application has the resources and database configuration(s) it needs to succeed. DBAs are not needed for the entire lifecycle of the project, however they should never lose sight of the project, nor should they take a back seat to the on-going management and maintenance of the solution post-production. DBAs will be called upon many times during the project to validate, verify, adjust or build database-specific components throughout the project as well as post-production. Constructing database views, building complex SQL queries are often required by our customers.

Programmers (UI/UX) – In many cases the customer has an existing IAM deployment (either from another vendor or a homegrown solution). In either case, the programmers that wrote the code and have maintained it since can provide valuable insight to the project team as to why the current solution is constructed the way it is. In many cases the goal of introducing a new IAM vendor is to revisit the configuration and "make it easier", and often times the programmers are required to contribute to the discussion and offer valuable intelligence as to why things are the way they are now. Programmers are sometimes crucial to the role out of Fischer or simply brought in to answer key questions when needed. UI / UX talent is applicable if the customer decides to modify the front-send self-service user interface. This will require java scripting & XHTML qualifications.

C-ICD-007	Implementation Costs and Details	Please provide a breakdown of the costs associated with delivering and implementing the solution for each phase and stage.	<p>Deployment Models</p> <p>Fischer offers its IdM capabilities in either an on-campus deployment or using Fischer's Identity as a Service® Cloud, a software-as-a-service (SaaS) model. On-campus deployments are ideal for institutions that prefer self-administration and management and desire to extend the solution without vendor professional services. On-campus deployments are generally sold with a perpetual software license for a specified number of users, and this model has a base annual maintenance fee of 22%. Hosted/Managed deployment in Fischer's Identity as a Service® Cloud enables institutions to outsource their IAM infrastructure and administration activities. For an annual subscription fee, Fischer performs all daily activities and provides a given number of hours of monthly services for performing routine tasks. The IaaS® option provides a term license for five (5) years for a specified number of users; a shorter term may be requested but may affect the price. Total Implementation Costs Based on the preliminary technical data provided by the institution, and additional population data retrieved from IPEDS and SCHEV, the following estimated implementation costs are provided:</p> <p>On Premise Deployment: \$112,000.00  Identity as a Service Deployment: \$110,775.00</p>
C-ICD-008	Implementation Costs and Details	Please provide a price breakdown for the proposed staffing plan including staff level / skillset, level of effort (i.e. hours), hourly rate of each resource, etc.	Please see Attachment E - VCU FTE Pricing Model
C-ICD-009	Total Cost	Include all costs for the solution offered in C-SMC--001 to C-SMC-005 and/or C-ICD-001 to C-ICD-008. The proposal prices shall include all costs for the products and services including all applicable freight and travel and living expensed; extra charges will not be allowed.	Please see Attachment E - Pricing Methodology.

Security Requirements for Data

Reference	Category	Question	Answer
T-SD-001	Security of Data (On-Premise)	Must have ability to operate on commercially supported and up-to-date hardware and software platforms.	Fischer Identity meets this requirement.
T-SD-002	Security of Data (On-Premise)	Must have ability for product vendor to promptly issue patches to address any known security vulnerabilities with any components of the product.	Fischer release in the Agile model with continuous integration. For on premise deployments, our goal is 1 major release per year with 2 or 3 service packs to tweak features and add any smaller enhancements. Security patches vary and may be applicable at any time.
T-SD-003	Security of Data (On-Premise)	Must have ability to have tiered user management architecture, where individual accounts can have different roles and different privileges associated with them.	Fischer Identity meets this requirement.
T-SD-004	Security of Data (On-Premise)	Must have ability to obfuscate and preferably encrypt selected data tuples or columns stored in the database.	We use an AES 128-bit encryption algorithm to encrypt data. This encryption is good for very strong obfuscation.
T-SD-005	Security of Data (On-Premise)	Must have ability to encrypt data in transit to other systems.	All communications is over SSL using Fischer published certificates.
T-SD-006	Security of Data (On-Premise)	Must have ability to audit and log user and system activities, and provide such information for ingestion by central log collection sources (such as syslog servers or eventing servers) and / or SIEM.	Fischer provides multiple user interface screens such as provisioning events, self-service events, etc that can provide administrators with a specific audit trail for a specific user, for a specific process or point in time. This feature is highly effective in troubleshooting identity/account issues. Furthermore all workflow instance files can be logged so administrators can view the data from a specific workflow process and not have to dig through large log files for answers. Third party tools such as Nagios, Splunk, etc. can be integrated for external monitoring and SIEM integration as required by the granularity of the customer's monitoring requirements.

Fischer Response to VCU RFP For Indentity and Access Management

T-SD-007	Security of Data (On-Premise)	Must have ability to provide multi-factor authentication for system access.	Fischer supports multi-factor authentication to both the Fischer application and to our Identity Provider. This means that users who are configured to use multi-factor authentication and try to access an application configured for SSO, they will be prompted for the 2nd factor before the open session is created. Fischer Identity supports provisioning and two-factor authentication using its own SMS and email based PIN verification, Duo Security, RSA SecurID, and time-based one time pin.
T-SD-008	Security of Data (On-Premise)	Must have ability to implement inactivity time-out for the system sessions, so inactive user sessions will be automatically dropped following pre-defined period of time.	Fischer Identity meets this requirement.
T-SD-009	Security of Data (On-Premise)	Must have ability to customize authentication controls, including password strength, expiration period, lockout threshold, lockout time, If unable to use single sign on through another authentication system	Fischer Identity meets this requirement.
T-SD-010	Security of Data (On-Premise)	Should use LDAP or SAML based single sign-on for access to system.	Fischer Identity utilizes Shibboleth Identity Provider to offer single sign-on into internal and hosted applications. Applications setup with a Service Provider (SP) for SAML can be integrated. Fischer also has mechanisms to connect to non SAML enabled applications.
T-SD-011	Security of Data (On-Premise)	Should be compatible with VCU's antivirus or other equivalent protection against malicious code.	Fischer Identity uses Ajax along with Richfaces for single page user experience. Various security tools were used to evaluate security flaws in Fischer Identity and as of now there is no known issue. Fischer Identity have been aggressively tested for Cross Site Scripting (XSS), SQL Injection and Ajax bridging (not used in Fischer Identity) and fixed all reported issues.

Fischer Response to VCU RFP For Identity and Access Management

T-SD-012	Security of Data (On-Premise)	Should protect against or ability to integrate with third party tools (such as Web Application firewalls and Database firewalls) that detect and protect against database level attacks.	Fischer has the ability to integrate with most all applications. Home grown applications that either function off of a core set of stored procedures (which Fischer is capable of calling) or a combination of web services and other standardized mechanisms (such as JDBC). The fluidity of Fischer's architecture provides us with the capability to integrate with just about any application that is capable of third party communication.
T-SD-013	Security of Data (On-Premise)	Should generate custom auditing events based on actions performed by individual user identities.	Fischer provides an accessible audit store that contains information about all user changes, so that everyday changes are audited from the store rather than from logs. Fischer's reporting engine comes with approximately 100 reports out of the box and the ability to build custom reports using any data contained in the Identity Profile and audit logs. Through this mechanism, this requirement is fully supported.
T-SD-014	Security of Data (On-Premise)	Should integrate with DUO Security's multi-factor authentication solution for administrative access to the system.	Fischer also has a full integration with DUO Security's ( <a href="http://www.duosecurity.com">http://www.duosecurity.com</a> ) push notification based multifactor authentication method. Other multifactor authentication methods are currently in testing prior to integration.
T-SD-015	Security of Data (On-Premise)	Should record and granularly audit changes to file and content of database, and the ability to provide these audit events as ingestible items by a SIEM or central log collection source.	Fischer provides an accessible audit store that contains information about all user changes, so that everyday changes are audited from the store rather than from logs. Fischer Identity runs through the Apache Tomcat process and can output log files to a SIEM in the log4j format. There are no direct integrations with SIEM platforms at this time.
T-SD-016	Security of Data (Cloud)	If the solution is SaaS or hosted off-site, the service provider <b>must</b> complete a full third party service provider assessment prior to VCU's procurement of its service.	Fischer Identity agrees to this requirement.

Fischer Response to VCU RFP For Identity and Access Management

T-SD-017	Security of Data (Cloud)	If the solution is SaaS or hosted off-site, the service provider <b>must</b> provide relevant documentation and when available, attestation around its infrastructure, platform, and application security architecture. These documentation may include, but are not limited to, SOC / SSAE-16 reports, internal information security policy and requirements, recent assessment, penetration testing, and audit reports.	Fischer Identity meets this requirement. Please see Attachment D - SOC 2 Report.
----------	--------------------------	---	--

A. Specific Proposal Requirements:

1. Proposals should be as thorough and detailed as possible so that VCU may properly evaluate your capabilities to provide the required goods/services.
2. Proposed Price.
  - a. Complete the third tab of Schedule A with the requested pricing information. Schedule A must contain all costs for the proposed IAM solution. Additional charges shall not be allowed.

Proposed pricing is included in the third tab of Schedule A.

3. Complete the first, second and fourth tab of Schedule A to provide specific plans and approach for providing the proposed software and services for the IAM solution proposed. **Mandatory requirements are designated by the words shall or must and desirable services are designated by the words should or may.**

The first, second and fourth tab of Schedule A have been completed.

4. Does / Shall your company agree to comply with all of the Procurement Requirements in Section V.C.?

Yes, Fischer agrees to comply with the Procurement Requirements in Section V.C.

5. Utilization of the words "shall" or "must" in Schedule A and Section V., Statement of Needs indicates a mandatory requirement:

Does / Shall your company comply with mandatory requirements as presented in Schedule A and Section V., Statement of Needs?

Yes  X  No \_\_\_\_\_

If "NO," identify the specific requirement and the reason for non-compliance.

6. Utilization of the words "should" or "may" in Section V, Statement of Needs indicates a non-mandatory requirement.

Does / Shall your company comply the non-mandatory requirements as presented in Schedule A and Section V., Statement of Needs (i.e. "should" becomes "shall")?

Yes  X  No \_\_\_\_\_

If "NO," identify the specific requirement and the reason for non-compliance.

7. Submit information about the qualifications and experience that your company has to provide the required products and services.

- a. Describe the firm's qualifications and experience providing the required products and services during the last three (3) years. Information provided should include, but is not limited to, comparable accounts in higher education and the scope of the services. Include information for a minimum of three (3) similar accounts, describing the types of projects and the scope of the services provided. Please

include contact information with the name, address, email address and current phone number.

Provided below are representative samples of project management and technical staff.

Fischer has implemented full suite IAM (role based access control, automated provisioning/deprovisioning, password management, self service access request and single sign-on) using Banner and/or PeopleSoft as the System of Record to automatically manage multiple identity life cycles (student, faculty, staff, adjunct, contractor, alumnae, and combinations thereof) involving most or potentially all of the systems listed in the RFP.

Project scope for the references listed in Response # T-EXP-007 are listed below. Please refer to Attachment G – References for specific contact information.

Customer: Howard Community College

Detail: Automated provisioning/deprovisioning, role management, password reset/synch.

Customer: Frostburg State University

Detail: Password Reset and Synch, Automated Role and Account Mgmt., Self Service Access Request, Compliance & Audit

Customer: Maryland Institute College of Art

Detail: Password Reset and Synch, Automated Role and Account Mgmt., Self Service (Admin. Provisioning), Compliance & Audit

Customer: Pepperdine University

Detail: Password Management, Automated Role and Account Mgmt. (2016)  
System(s) of Record:

Customer: University of Maryland University College

Detail: Password reset for approx. 100K students worldwide. Over 600,000 users managed by IAM system. System of Record: PeopleSoft

Customer: Swarthmore College

Detail: Password Reset and Synch, Automated Role and Account Mgmt., Self Service (Admin. Provisioning), Compliance & Audit.

System of Record: Banner (BEIS)

User Base: Enrollment: 5,000; Total licenses: 55,000

- b. Specify any technicians your company intends to assign to the VASCUPP contract. Provide information to include but is not limited to the names, qualifications, and experience of the technicians to be assigned to the contract. Resumes of staff to be assigned to the contract may be used. Submit relevant professional certifications for the technicians proposed to work on contract projects.

Fischer reserves the right to assign or not assign a project manager based on the overall dynamic of the project team.

Fischer does not actively staff a project management group, rather we assign principal architects that stay attached throughout the solution. Depending on the timing of your project, will depend on which architect will be assigned to your project.



**Primary Contact**

[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]

[Redacted]

[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]

**Your IAM Architect**

Name        Bryan Leber  
Job Title    IAM Architect

[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- d. Provide a list of institutions of higher education with which your firm has a signed term contract.

CONFIDENTIAL: Of the references provided in RFP Response T-EXP-007, the following have term agreements: University of Maryland, University College, Frostburg State University, Howard Community College, Maryland Institute College of Art. Baylor University, Vassar, and many other institutions also have term contracts, however, Fischer policy prevents a full list of customers.

- e. Provide the amount of annual sales the firm has with each VASCUPP Member Institution. A list of VASCUPP Members can be found at:

<http://procurement.vcu.edu/our-services/university-purchasing/vascupp/>

\$0.00 Fischer International Identity LLC does not currently have any sales with VASCUPP Member Institutions.

8. Does your company accept the terms and conditions as presented in Section X, General Terms and Conditions and in Section XI, Special Terms and Conditions to govern the contract?

Yes  X  No \_\_\_\_\_

If "NO," identify the specific term and condition(s) and the reason for non-compliance.

10. Small, Women-Owned and Minority-Owned Business commitment for utilization.
- a. The Offeror must submit complete information on Appendix I unless the Offeror is a Department of Small Business and Supplier Diversity (DSBSD). DSBSD certified small businesses must include their certification number on the coversheet of this RFP, but are not required to complete Appendix I.

Appendix I is complete.

11. Method of Payment

- a. The Offeror must complete and submit Appendix II to select an electronic payment method.

Appendix II is complete

## APPENDIX I

### PARTICIPATION IN STATE PROCUREMENT TRANSACTIONS SMALL BUSINESSES AND BUSINESSES OWNED BY WOMEN AND MINORITIES

The following definitions will be used in completing the information contained in this Appendix.

#### Definitions

- **Small business** is an independently owned and operated business which, together with affiliates, has 250 or fewer employees, or average annual gross receipts of \$10 million or less averaged over the previous three years. Nothing in this definition prevents a program, agency, institution or subdivision from complying with the qualification criteria of a specific state program or federal guideline to be in compliance with a federal grant or program.
- **Women-owned business** is a business concern which is at least 51 percent owned by one or more women who are U.S. citizens or legal resident aliens, or in the case of a corporation, partnership or limited liability company or other entity, at least 51 percent of the equity ownership interest in which is owned by one or more women, and whose management and daily business operations are controlled by one or more of such individuals.
- **Minority-owned business** is a business concern which is at least 51 percent owned by one or more minorities or in the case of a corporation, partnership or limited liability company or other entity, at least 51 percent of the equity ownership interest in which is owned by one or more minorities and whose management and daily business operations are controlled by one or more of such individuals.
- **Minority Individual:** "Minority" means a person who is a citizen of the United States or a legal resident alien and who satisfies one or more of the following definitions:
  - "Asian Americans" means all persons having origins in any of the original peoples of the Far East, Southeast Asia, the Indian subcontinent, or the Pacific Islands, including but not limited to Japan, China, Vietnam, Samoa, Laos, Cambodia, Taiwan, Northern Marinas, the Philippines, U. S. territory of the Pacific, India, Pakistan, Bangladesh and Sri Lanka and who are regarded as such by the community of which these persons claim to be a part.
  - "African Americans" means all persons having origins in any of the original peoples of Africa and who are regarded as such by the community of which these persons claim to be a part.
  - "Hispanic Americans" means all persons having origins in any of the Spanish speaking peoples of Mexico, South or Central America, or the Caribbean Islands or other Spanish or Portuguese cultures and who are regarded as such by the community of which these persons claim to be a part.
  - "Native Americans" means all persons having origins in any of the original peoples of North America and who are regarded as such by the community of which these persons claim to be a part or who are recognized by a tribal organization.
  - "Eskimos and Aleuts" means all persons having origins in any of the peoples of Northern Canada, Greenland, Alaska, and Eastern Siberia and who are regarded as such in the community of which these persons claim to be a part.

PARTICIPATION BY SMALL BUSINESSES, BUSINESSES OWNED BY WOMEN  
BUSINESSES OWNED BY MINORITIES

This appendix should only be completed by firms that are not Virginia Department of Small Business and Supplier Diversity (DSBSD) certified small businesses.

Offeror certifies that it will involve Small Businesses, Women-Owned Businesses, and/or Minority-Owned Businesses (SWaM) in the performance of this contract either as part of a joint venture, as a partnership, as Subcontractors or as suppliers.

VCU has an overall goal of 42% SWaM participation for all annual purchases and seeks the maximum level of participation possible from all its contractors.

List the names of the SWaM Businesses your firm intends to use and identify the direct role of these firms in the performance of the contract. State whether the firm is a Small Business (SB), Women-Owned (WO), or Minority-Owned (MO).

<u>Name of Businesses:</u>	<u>SB, WO, MO:</u>	<u>Role in contract:</u>
None		

**Commitment for utilization of DSBSD SWaM Businesses:**  
0 % of total contract amount that will be performed by DSBSD certified SWaM businesses.

**Identify the individual responsible for submitting SWaM reporting information to VCU:**

Name Printed: N/A  
Email: \_\_\_\_\_  
Phone: \_\_\_\_\_  
Firm: \_\_\_\_\_

Offeror understands and acknowledge that the percentages stated above represent a contractual commitment by the Offeror. Failure to achieve the percentage commitment will be considered a breach of contract and may result in contract default.

Acknowledged:  
By (*Signature*): \_\_\_\_\_  
Name Printed: R. Andrew Sroka  
Title: Presidenty & CEO  
Email: ras@fischerinternational.com

Note: Small, Minority and/or Women-owned business sub-contractors are required to become certified and maintain certification through the Virginia Department of Small Business and Supplier Diversity (DSBSD; <http://www.sbsd.virginia.gov/swamcert.html> ) to fulfill the Offeror's commitment for utilization.

## APPENDIX II INVOICING AND PAYMENT

### Invoicing:

The Contractor shall submit a fully itemized invoice to Virginia Commonwealth University, Accounts Payable and Support Services, P. O. Box 980327, Richmond, VA 23298-0327, that, at minimum, includes the following information: the Virginia Commonwealth University purchase order number; a description of the goods or services provided; quantities; unit prices; extended prices; and total prices. Payment will be issued in accordance with the payment method selected below and with the Commonwealth of Virginia Prompt Payment Legislation.

Upon request by VCU, the Contractor shall submit invoices electronically using the Ariba Network or other e-commerce channel utilized by VCU; and agrees to comply, within reason, with any future e-commerce initiatives including, but not limited to: procurement, procurement content, sourcing or any other electronic procurement and sourcing solutions.

Questions regarding this method of invoicing should be sent to: [ecommerce@vcu.edu](mailto:ecommerce@vcu.edu).

### Payment:

VCU Procurement Services is automating the payment process to the greatest extent possible. Contractors are encouraged to accept payment electronically through the commercial card program. Please review the payment methods described below and select one for your firm. By selecting the payment method below, Contractor acknowledges that the selected payment method is **not specific to the contract resulting from this solicitation and will apply to all payments made to the Contractor** by Virginia Commonwealth University. For example, if the Contractor has an existing contract(s) and is currently receiving payment by paper check, and the Contractor is now electing to receive payment by the commercial card, **all payments** will be made using the commercial card once the commercial card payment process is implemented for the firm.

#### **Payment Methods**

**1. Electronically through a Wells Fargo Visa commercial card:** Payment will be made ten days (10) after receipt of a proper invoice for the amount of payment due, or ten (10) days after receipt of the goods or services, whichever is later.

It is the Contractor's responsibility to contact its banking institutions to determine any credit limit that may restrict the payment of invoices. It is the Contractor's responsibility to have its credit limit raised as necessary to facilitate the timely payment of all invoices. Invoices exceeding the Contractor's credit limit will be returned unpaid.

Failure to accept the commercial card after award of contract will be considered a contract compliance issue and will be addressed accordingly. In addition, invoices will be returned without payment until the Contractor can accept the payment through the commercial card.

Questions regarding this method of payment should be sent to [commcard@vcu.edu](mailto:commcard@vcu.edu).

2. **ACH:** Electronic payment via automated clearing house (ACH) to the vendor provided bank account of record. Payment is processed thirty (30) days after receipt of a proper invoice for the amount of payment due, or thirty (30) days after receipt of the goods or services, whichever is later. Additional information about ACH payments is available at: <http://www.vcu.edu/treasury/VendorACH.htm>.

**Contractor must indicate the method of payment selected:**

Commercial Card Payment (Wells Fargo VISA)  
 Automated Clearing House (ACH)

**Invoicing and Payment Method Acknowledgement:**

Signature:	_____
Name Printed:	R. Andrew Sroka
Title:	President & CEO
Name of Firm:	Fischer International Identity, LLC
Date:	November 15, 2016

Please identify the following contact information for the individual who will serve as the appropriate point of contact within your company to be contacted by VCU Accounts Payable to implement the electronic invoicing and payment processes:

Name of the individual:	Jane Rice
Title:	Accounts Payable
Mailing address:	9045 Strada Stell Court # 200 Naples, FL 34109
Email address:	jer@fischerinternational.com
Phone number:	706 922 1408
Fax number:	239 436-2555

Fischer International Identity  
9045 Strada Stell Ct  
Naples, Florida 34109  
+1 239-643-1500  
[www.FischerInternational.com](http://www.FischerInternational.com)



Identity Management Made for  
Higher Education™

Copyright © 2005-2016 Fischer International Identity, LLC. All rights reserved.  
Fischer International, Fischer International Identity, Managed Identity Services, Managed Identity Services Technology, Identity as a Service, IaaS, the Fischer International Logo, Global Identity Architecture, Built for Business... Yours, Ignite-IT, and all other Fischer product or service names are the trademarks and/or registered trademarks of Fischer International Identity.



## APPENDIX I

### PARTICIPATION IN STATE PROCUREMENT TRANSACTIONS SMALL BUSINESSES AND BUSINESSES OWNED BY WOMEN AND MINORITIES

The following definitions will be used in completing the information contained in this Appendix.

#### Definitions

- **Small business** is an independently owned and operated business which, together with affiliates, has 250 or fewer employees, or average annual gross receipts of \$10 million or less averaged over the previous three years. Nothing in this definition prevents a program, agency, institution or subdivision from complying with the qualification criteria of a specific state program or federal guideline to be in compliance with a federal grant or program.
- **Women-owned business** is a business concern which is at least 51 percent owned by one or more women who are U.S. citizens or legal resident aliens, or in the case of a corporation, partnership or limited liability company or other entity, at least 51 percent of the equity ownership interest in which is owned by one or more women, and whose management and daily business operations are controlled by one or more of such individuals.
- **Minority-owned business** is a business concern which is at least 51 percent owned by one or more minorities or in the case of a corporation, partnership or limited liability company or other entity, at least 51 percent of the equity ownership interest in which is owned by one or more minorities and whose management and daily business operations are controlled by one or more of such individuals.
- **Minority Individual:** "Minority" means a person who is a citizen of the United States or a legal resident alien and who satisfies one or more of the following definitions:
  - "Asian Americans" means all persons having origins in any of the original peoples of the Far East, Southeast Asia, the Indian subcontinent, or the Pacific Islands, including but not limited to Japan, China, Vietnam, Samoa, Laos, Cambodia, Taiwan, Northern Marinas, the Philippines, U. S. territory of the Pacific, India, Pakistan, Bangladesh and Sri Lanka and who are regarded as such by the community of which these persons claim to be a part.
  - "African Americans" means all persons having origins in any of the original peoples of Africa and who are regarded as such by the community of which these persons claim to be a part.
  - "Hispanic Americans" means all persons having origins in any of the Spanish speaking peoples of Mexico, South or Central America, or the Caribbean Islands or other Spanish or Portuguese cultures and who are regarded as such by the community of which these persons claim to be a part.
  - "Native Americans" means all persons having origins in any of the original peoples of North America and who are regarded as such by the community of which these persons claim to be a part or who are recognized by a tribal organization.
  - "Eskimos and Aleuts" means all persons having origins in any of the peoples of Northern Canada, Greenland, Alaska, and Eastern Siberia and who are regarded as such in the community of which these persons claim to be a part.

PARTICIPATION BY SMALL BUSINESSES, BUSINESSES OWNED BY WOMEN  
BUSINESSES OWNED BY MINORITIES

This appendix should only be completed by firms that are not Virginia Department of Small Business and Supplier Diversity (DSBSD) certified small businesses.

Offeror certifies that it will involve Small Businesses, Women-Owned Businesses, and/or Minority-Owned Businesses (SWaM) in the performance of this contract either as part of a joint venture, as a partnership, as Subcontractors or as suppliers.

VCU has an overall goal of 42% SWaM participation for all annual purchases and seeks the maximum level of participation possible from all its contractors.

List the names of the SWaM Businesses your firm intends to use and identify the direct role of these firms in the performance of the contract. State whether the firm is a Small Business (SB), Women-Owned (WO), or Minority-Owned (MO).

Name of Businesses:

SB, WO, MO:

Role in contract:

<u>Name of Businesses:</u>	<u>SB, WO, MO:</u>	<u>Role in contract:</u>
None		

**Commitment for utilization of DSBSD SWaM Businesses:**

0 % of total contract amount that will be performed by DSBSD certified SWaM businesses.

**Identify the individual responsible for submitting SWaM reporting information to VCU:**

Name Printed: N/A  
Email: \_\_\_\_\_  
Phone: \_\_\_\_\_  
Firm: \_\_\_\_\_

Offeror understands and acknowledge that the percentages stated above represent a contractual commitment by the Offeror. Failure to achieve the percentage commitment will be considered a breach of contract and may result in contract default.

Acknowledged:  
By (*Signature*): \_\_\_\_\_  
Name Printed: R. Andrew Sroka  
Title: Presidenty & CEO  
Email: ras@fischerinternational.com

Note: Small, Minority and/or Women-owned business sub-contractors are required to become certified and maintain certification through the Virginia Department of Small Business and Supplier Diversity (DSBSD; <http://www.sbsd.virginia.gov/swamcert.html>) to fulfill the Offeror's commitment for utilization.

## APPENDIX II INVOICING AND PAYMENT

### Invoicing:

The Contractor shall submit a fully itemized invoice to Virginia Commonwealth University, Accounts Payable and Support Services, P. O. Box 980327, Richmond, VA 23298-0327, that, at minimum, includes the following information: the Virginia Commonwealth University purchase order number; a description of the goods or services provided; quantities; unit prices; extended prices; and total prices. Payment will be issued in accordance with the payment method selected below and with the Commonwealth of Virginia Prompt Payment Legislation.

Upon request by VCU, the Contractor shall submit invoices electronically using the Ariba Network or other e-commerce channel utilized by VCU; and agrees to comply, within reason, with any future e-commerce initiatives including, but not limited to: procurement, procurement content, sourcing or any other electronic procurement and sourcing solutions.

Questions regarding this method of invoicing should be sent to: [ecommerce@vcu.edu](mailto:ecommerce@vcu.edu).

### Payment:

VCU Procurement Services is automating the payment process to the greatest extent possible. Contractors are encouraged to accept payment electronically through the commercial card program. Please review the payment methods described below and select one for your firm. By selecting the payment method below, Contractor acknowledges that the selected payment method is **not specific to the contract resulting from this solicitation and will apply to all payments made to the Contractor** by Virginia Commonwealth University. For example, if the Contractor has an existing contract(s) and is currently receiving payment by paper check, and the Contractor is now electing to receive payment by the commercial card, **all payments** will be made using the commercial card once the commercial card payment process is implemented for the firm.

### **Payment Methods**

**1. Electronically through a Wells Fargo Visa commercial card:** Payment will be made ten days (10) after receipt of a proper invoice for the amount of payment due, or ten (10) days after receipt of the goods or services, whichever is later.

It is the Contractor's responsibility to contact its banking institutions to determine any credit limit that may restrict the payment of invoices. It is the Contractor's responsibility to have its credit limit raised as necessary to facilitate the timely payment of all invoices. Invoices exceeding the Contractor's credit limit will be returned unpaid.

Failure to accept the commercial card after award of contract will be considered a contract compliance issue and will be addressed accordingly. In addition, invoices will be returned without payment until the Contractor can accept the payment through the commercial card.

Questions regarding this method of payment should be sent to [commcard@vcu.edu](mailto:commcard@vcu.edu).

2. **ACH:** Electronic payment via automated clearing house (ACH) to the vendor provided bank account of record. Payment is processed thirty (30) days after receipt of a proper invoice for the amount of payment due, or thirty (30) days after receipt of the goods or services, whichever is later. Additional information about ACH payments is available at: <http://www.vcu.edu/treasury/VendorACH.htm>.

**Contractor must indicate the method of payment selected:**

Commercial Card Payment (Wells Fargo VISA)  
 Automated Clearing House (ACH)

**Invoicing and Payment Method Acknowledgement:**

Signature:	_____
Name Printed:	R. Andrew Sroka
Title:	President & CEO
Name of Firm:	Fischer International Identity, LLC
Date:	November 15, 2016

Please identify the following contact information for the individual who will serve as the appropriate point of contact within your company to be contacted by VCU Accounts Payable to implement the electronic invoicing and payment processes:

Name of the individual:	Jane Rice
Title:	Accounts Payable
Mailing address:	9045 Strada Stell Court # 200 Naples, FL 34109
Email address:	jer@fischerinternational.com
Phone number:	706 922 1408
Fax number:	239 436-2555

## ***Attachment A***

### ***Fischer International Identity***

IDENTITY MANAGEMENT FOR HIGHER EDUCATION™

Answer to questions T-IT-071, PS-APP-008 and C-ICD-005.

## Fischer Implementation Project Methodology

# Fischer Implementation Project Methodology

## Executive Summary:

Fischer has developed a project methodology that ensures customer solutions are built on-time, within budget, and to the customer's business and technical requirements. The purpose of this document is to provide the reader with an understanding as to how Fischer can consistently deliver quality and predictable IdM implementations and in timeframes that are drastically shorter than conventional IdM projects. This document begins with a discussion of our approach and is followed by an overview of the phases in which customer solutions are planned, designed, and implemented.

## Accelerated Solution Delivery:

Fischer International Identity advocates and utilizes the agile project management methodology. As with any implementation, the X factor is the preparation, agreement and understanding of the requirements and solution specifications as well as ensuring the pre-requisites are met to install the product and ultimately build a solution. This process will take as long as is required, and the responsibility primarily lies with the customer pertaining to the defining and publishing the official solution requirements. It is important to note that our project timeline focuses on our ability to provide the required solution and not on the logistical hurdles that may occur. Our approach to projects drastically limits the liability associated with scope creep and validating prerequisites are met prior to engaging our technical team to actually perform the implementation. We've found this approach to streamline the solution construction phases.

As an organization we do not focus our project plan on unintended delays nor do we anticipate failure. We do understand that those things happen and we are not naive to this important point; however we address those items at the proper time and with the proper people involved. For example, a daily standup meeting is scheduled at the beginning of the project. This meeting will stay in place for the duration of the project. The goal of this meeting is to ensure forward progress on the project and discuss any impediments that are blocking the project's ability to move forward. We cannot predict delays from a project timeline perspective; rather mitigate them when they arise. We focus on how long it will take our team to deploy your solution using our product with agreement on the requirements and design. We understand that this part of the process is time consuming and can be frustrating, and that is why we do not commit project resources beyond a project manager and the implementation manager during this phase of the project. We want to focus on making sure the scope is defined and the requirements are understood and accepted internally, before you publish them to Fischer.

Once the requirements are published, we will review and ask any clarifying questions that may arise to ensure we have an intimate understanding of your goals and project requirements.

We will then create a preliminary solution design document consisting of the following:

- a. A "statement of understanding" related to how well the implementation engineer understands the customer's requirement (based on the information available).
- b. A high-level data flow diagram as a representation of the customer's responses to the Solution Questionnaire Packet (SQP), depicting anticipated source of authority for identity, all downstream target systems, and the [known] beneficiaries (which may not be right).
- c. A graphical representation of the design specification pertaining to how the Fischer product will solve the problem. The following specifications are required:

- i. Recommended event detection method (real-time or near-real-time)
- ii. Data requirements for policy evaluation [if available]
- iii. Diagram showing the flow of the data through the Fischer solution (i.e. trigger → policy evaluation → target workflow execution, notifications).

This approach gives the project team the ability to first focus on validating our understanding of your requirements while also focusing on the areas your team sees as a lack of understanding on our part, or potentially flag a requirement that was not provided or may have been described inadequately. This approach will help to ensure a sound and proper understanding of your solution requirements before we begin the implementation.

What is NOT in the project plan is the amount of time that will pass between the workshop and the acceptance of the requirements document, nor how long it may take customers to perform proper user acceptance testing.

We also offer a streamlined approach to a well-known project problem; delays in SOW signoff due to the need to review in detail before the customer signs. Our goal is to complete the statement of work at the workshop to enable the customer to have direct access to the author in an effort to provide all clarification immediately, and enable sign-off during the workshop. We understand this is an aggressive approach; however we are confident it is the model and approach that is in the best interest of our customers. However it does require active and aggressive engagement from the customer's project team, and on a daily basis. We do have other approaches to projects that can be employed if the agile method is too aggressive, however we strongly recommend the agile approach given the success we've seen employing it.

Other approaches include elongated timelines and more of a waterfall approach. We are not confident in such models nor are we able to commit to a firm project deadline if employed. We have employed the waterfall method in the past and the result is delays, delays and more delays. Frustration generally grows out of a waterfall model, primarily because of the surprises that surface from a requirements perspective. We've found the agile approach to be more predictable, faster, easier, and a much more appropriate model for deployment solutions.

It is important to note that Fischer is trained in the agile model, and our scrum master can make sure the team follows all the guidelines and principals required to successfully execute the project.

## Fischer Project Implementation: Project Phases

Note that our proposed implementation timeline (provided previously) focuses on Phases V and VI, as that is the actual phase where we will provide the implementation services. Phases I, II & III require customer's to take the majority of the action. Any delay from the customer will result in a delay to the timeline.

Phase	Focus	Description	Duration
Phase I	Project logistics and meeting structure	<p>This is the initiation point of all implementation projects. During this phase, the project managers / leads will begin meeting on a daily basis to discuss the project and define the plan.</p> <p>Key milestones for this phase include:</p> <ul style="list-style-type: none"> <li>• Define the meeting structure</li> <li>• Present Fischer's project methodology and underlying process to the customer</li> <li>• Review and distributing the Solution Questionnaire Packet (SQP)</li> </ul> <p>During this phase, the project managers / leads will begin meeting on a daily basis to discuss the project and define the plan.</p>	This phase is typically handled in 2 meetings.
Phase II	Requirements gathering	<p>The goal of this phase is to validate the customer's business and technical requirements. This phase does not focus on performing technical tasks related to the solution, rather it centers on collaboration between Fischer and the customer and building the team of resources that will be required to successfully complete the project.</p> <p>Key milestones for this phase include:</p> <ul style="list-style-type: none"> <li>• Complete Solution Questionnaire Packet (<i>by customer</i>)</li> <li>• Complete Use Case Definitions /"user stories" (<i>by customer</i>)</li> <li>• Schedule Workshop</li> <li>• Complete Solution Workshop (resulting in a Statement of Work)</li> <li>• Assign Implementation Team</li> <li>• Select Project Due Date</li> </ul> <p><i>NOTE: historically, this is the phase where IdM projects slow down and cause delays primarily due to lack of a defined requirement specification to the level of detail required. It is important to note that this phase is designed to produce a detailed specification which will avoid such delays. The requirements phase can span as much as 30 days (or it can be completed during the workshop week if the customer provides the required resources to fully define the requirements).</i></p>	1 week if customer is well prepared; up to 30 days otherwise.



Phase III	Platform installation and configuration	<p>This phase begins the technical portion of the project. During this phase, the platform is discussed and configured according to the requirements document as defined by Fischer, which will meet or exceed the platform / infrastructure specifications for a successful deployment and on-going support of the customer's business processes and underlying transactional load.</p> <p>This phase requires the customer to provide personnel directly responsible for building the platform. Typically this will be network administrators, MIS professionals, application analysts, etc. Essentially, whoever is responsible for installing operating systems, configuring web servers, and installing the required 3<sup>rd</sup> party components must be available during this phase.</p> <p><i>Note: Fischer Operational Consultants are available to answer questions during this phase without additional cost. Charges will apply if Consultants are requested to assist with configuration or completion of milestones within this phase. Such activities must be first documented in the Statement of Work.</i></p>	1 – 3 days if customer is prepared and/or makes platform installation a priority
Phase IV	Network Configuration	<p>During this phase, the customer is responsible for configuring all network devices per the specifications required by the Fischer product. The specifications are provided in the requirements document and must be met during this phase. Additionally, the customer will provide personnel directly responsible for building the platform. Typically this will be information security, network administrators, firewall administrators, MIS professionals, application analysts, etc.</p> <p>Key milestones for this phase include:</p> <ul style="list-style-type: none"> <li>• Configure Firewall</li> <li>• Configure SSL</li> <li>• Configure Load balancer <i>(if applicable)</i></li> </ul> <p><i>Note: Fischer Operational Consultants are available to answer questions during this phase without additional cost. Charges will apply if Consultants are requested to assist with configuration or completion of milestones within this phase. Such activities must be first documented in the Statement of Work.</i></p>	1 – 3 days if customer is prepared and/or makes network configuration a priority
Phase V	Application tier install / configuration	<p>The goal of this phase is to install the Fischer product and verify communications. The installation parameters will change depending upon key environment components (i.e. Windows vs. Unix) as well as the purchased service model (IaaS® or on premise).</p> <p>Key milestones for this phase include:</p> <ul style="list-style-type: none"> <li>• Install Fischer product</li> <li>• Test Communications</li> </ul>	1 day in most cases. Note that this phase cannot begin until phases III and IV are complete.

		<i>Note: The customer may install the Fischer product, independent of Fischer, if desired. If the Fischer implementation team is required to install the software, additional charges will apply and must be first documented in the Statement of Work.</i>	
Phase VI	Solution construction	<p>The goal of this phase is to build to solution as defined by the Statement of Work and requirements document.</p> <p>Key milestones for this phase include:</p> <ul style="list-style-type: none"> <li>• Complete solution requirements in test environment</li> <li>• Build production environment</li> </ul>	Varies based on IdM modules. E.g., 4 weeks for full-suite project with 5 Fischer resources.
Phase VII	User acceptance testing	<p>The goal of this phase is for the customer to validate that the solution meets all defined technical and business requirements.</p> <p>The customer will test the solution independent of Fischer personnel and report back to the team during the daily standup meeting. The daily standup should remain limited to 15 minutes and, if breakout meetings are required, they can be scheduled at this time.</p>	1 – 2 weeks.
Phase VIII	Production migration	<p>During this phase, the solution will be migrated to production and re-tested. A final solution acceptance will result from a successful completion of this phase.</p> <p>Key milestones for this phase include:</p> <ul style="list-style-type: none"> <li>• Test Solution (<i>by customer</i>)</li> <li>• Accept Solution (<i>by customer</i>)</li> </ul>	4 days
Phase IX	Solution Presentation	<p>The goal of this phase is to present the delivered solution to customer's project team participants and all applicable business units. The Fischer Implementation Lead will take all attendees on a tour of the solution from beginning to end, covering all pertinent details to ensure knowledge gaps are limited.</p>	1 day
Phase X	Solution Turnover	<p>The goal of this phase is to turn-over the solution to the appropriate personnel to begin providing post-production acceptance support.</p> <p>Key milestones for this phase include:</p> <ul style="list-style-type: none"> <li>• Deliver Solution Documentation</li> <li>• Perform Post Implementation Services (<i>if purchased</i>)</li> <li>• IaaS® Support Turnover, if applicable</li> </ul>	1 day

Fischer International Identity, LLC  
9045 Strada Stell Court, Suite #201  
Naples, FL 34109  
239-643-1500  
[www.FischerInternational.com](http://www.FischerInternational.com)



**IDENTITY MANAGEMENT FOR HIGHER EDUCATION™**

©2015 Fischer International Identity, LLC. All rights reserved.  
Fischer International, Fischer International Identity, Managed Identity Services, Identity as a Service, IaaS, the Fischer International Logo, Global Identity Architecture, DataForum, Fischer Global Provisioner, Built for Business...Yours, and all other Fischer product or service names are the trademarks and/or registered trademarks of Fischer International. All other company, product, or trade names are the property of their respective owners.

# Attachment B

## *Fischer International Identity*

Identity Management for Higher Education

Answer to question T-ARCH-043 and T-IOM-033

# Fischer Identity™ V5.3

## Official Project Pre-Requisites Guide

## Fischer Hardware and Software Requirements

Fischer Identity enables you to choose either traditional commercial operating systems (Windows, Solaris) or Linux open-source platforms. Choosing an open-source operating system, application server and data stores may help you realize a lower TCO and more rapid time to value by avoiding the cost of user licenses.

Fischer Identity also enables you to choose procurement models: on-premise or SaaS (Fischer Identity as a Service® cloud). Fischer Identity as a Service cloud provides a high-availability environment and Fischer typically recommends a high-availability environment for on-premise, though this is not required. When high availability is selected, at least two servers are required. The operating environment can consist of hardware or a VMware environment.

### On-Premise

For hardware in an on-premise implementation, you can choose Windows or UNIX operating environments. The requirements for each environment are listed below:

Fischer's installation guide provides the minimum requirements to install Fischer Identity. The following hardware specifications take into account a production solution for up to 30,000 users with event-driven and request-based provisioning, password management, an active compliance implementation, enterprise business roles, approvals, and an audit database.

These assumptions should be taken into account when reviewing the hardware recommendations:

- The hardware requirements specified in this document assume a sole tenancy, dedicated environment per client. The hardware specifications are not the recommended approach in the Service Provider (Hosted) model.\*
- The hardware requirements specified pertain to the amount of memory, disk space and CPU usage the Fischer Suite will utilize at each layer.
- The hardware requirements specified in this document do not take into account the possibility that a service provider may potentially “multi-task” each layer or tier. This means that the Fischer Suite might not be the only application utilizing server resources at any level (Web Tier, Application Tier, Data Tier).
- We recommend further research with your platform vendor at each layer. For example, if you are using Microsoft IIS at the web layer, Fischer recommends that you verify that the hardware requirements for the Fischer server also fall in line with what Microsoft recommends for their product. This statement holds true for all layers and platform vendors. In short, the recommendations below are for the Fischer product only and do not account for specific vendor requirements above and beyond those that may potentially be required by Fischer. Specific vendor requirements may increase the hardware specifications at each layer.

- This document is valid for the Intel platform only. SPARC specifications can be provided upon request.

*\* In a service provider (hosted) model, Fischer recommends virtualization as a standard approach. Virtualization has the potential of decreasing hardware costs, and consolidating (people) resources for Administration.*

Tier	CPU	RAM	HDD
Web Server	(x2) Intel quad-core	4GB up to 8GB	100GB
Application Tier	(x2) Intel quad-core	4GB up to 8GB	200GB
Data Tier	(x2) Intel quad-core	4GB up to 8GB	200GB

## Identity & Provisioning Servers / UNIX Installation Prerequisites

<b>Operating system</b>	UNIX, Linux, Solaris 10 or later.
<b>Java support</b>	Sun Java Development Kit (JDK) 1.7.60
<b>Communications</b>	TCP/IP on UNIX for browser connectivity to Web server.
<b>Identity Directory Server Store</b>	Ensure that one of these directory servers has been installed and that an LDAP port has been enabled for the directory: <ul style="list-style-type: none"> <li>• 389 Directory Server (formerly called Fedora Directory Server) 1.3.x</li> <li>• Open LDAP</li> <li>• OpenDJ version 2.4 or later</li> <li>• Red Hat Directory Server</li> </ul>
<b>Application server</b>	Apache Tomcat Web application server Version 7.0.54, which is available on the IdM Suite Software folder\Additional Software\UNIX.
<b>Web Server</b>	Apache HTTPD
<b>Product/Audit/ Dashboard databases</b>	One of these databases: <ul style="list-style-type: none"> <li>• Oracle Version 11g or later.</li> <li>• PostgreSQL 9.2 or later.</li> <li>• Microsoft SQL Server Version 2012 or later.</li> </ul>

### Linux OS Tuning:

Modify the following files as shown below and restart the servers.

#### **/etc/sysctl.conf**

```
fs.file-max = 64000
```

**/etc/security/limits.conf** (Settings can be limited to the users listed above instead of \*, everybody)

```
* soft nofile 54000
* hard nofile 54000
* soft nproc 54000
* hard nproc 54000
```

Some flavors of Linux have an additional file that overrides what you set in the `/etc/security/limits.conf`. If you have `/etc/security/limits.d/90-nproc.conf`, this will set the soft `nproc` value to 1024. Go ahead and comment out that line in the `/etc/security/limits.d/90-nproc.conf`

Set the following ulimit for all the above users:

```
ulimit -u 8192
ulimit -n 8192
```

```
[iaas3df3@520696-prov3 logs]$ ulimit -a
core file size          (blocks, -c) 0
data seg size          (kbytes, -d) unlimited
scheduling priority    (-e) 0
file size              (blocks, -f) unlimited
pending signals        (-i) 514848
max locked memory      (kbytes, -l) 64
max memory size        (kbytes, -m) unlimited
open files             (-n) 8192
pipe size              (512 bytes, -p) 8
POSIX message queues   (bytes, -q) 819200
real-time priority     (-r) 0
stack size             (kbytes, -s) 10240
cpu time               (seconds, -t) unlimited
max user processes     (-u) 8192
virtual memory         (kbytes, -v) unlimited
file locks             (-x) unlimited
```

Once all these configurations have been done it is recommended to restart the server and apache tomcat to ensure it takes the new settings.

Note: Fischer recommends using the ext4 file system with all flavors of Linux.

## Identity & Provisioning Server Windows Installation Prerequisites

### Software Requirements

<b>Operating system</b>	One of these 64-bit version operating systems: Windows Server 2008 R2, 2012, 2012 R2 or later.
<b>Java support</b>	Sun Java Development Kit (JDK) 1.7.60 or later. If not already installed, depending upon your operating system, use 64-bit version from the IdM Suite Software folder\Additional Software\Windows\Java. Point the JAVA_HOME environment variable to the JDK installation directory, for example, C:\Program Files\Java\jdk1.7.0_60 for 64-bit.
<b>Application server</b>	Apache Tomcat Web application server Version 7.0.54 (included with the IdM Suite installation). <b>Notes:</b> <ul style="list-style-type: none"> <li>• The Web application server must run under an administrative account to perform certain functions: <ul style="list-style-type: none"> <li>- To reset the password of a user in Microsoft Active Directory</li> <li>- To use the Windows Command Line connector</li> </ul> </li> </ul> This account can be a member of the local Administrators group or a member of the domain Administrators group <ul style="list-style-type: none"> <li>- You must use same level (64-bit) for both Java and Apache Tomcat.</li> </ul>
<b>Web Server</b>	Windows Internet Information Sharing (IIS)
<b>Identity Directory Server Store</b>	Ensure that one of these directory servers has already been installed and that an LDAP port has been enabled for the directory: <ul style="list-style-type: none"> <li>• OpenDJ version 2.4 or later.</li> <li>• Microsoft Active Directory 2008 R2, 2012, 2012 R2 or later.</li> <li>• 389 Directory Server (formerly called Fedora Directory Server) 1.3.x</li> <li>• Red Hat Directory Server</li> <li>• Open LDAP</li> </ul>
<b>Product/Audit/Dashboard databases</b>	One of these databases: <ul style="list-style-type: none"> <li>• Oracle Version 11g or later.</li> <li>• Microsoft SQL Server Version 2012 or later.</li> <li>• PostgreSQL 9.2.x or later.</li> </ul>
<b>Web browser</b>	Admin UI: Microsoft Internet Explorer 9.0 or later. Self-Service UI: Microsoft Internet Explorer 9.0 or later, Mozilla Firefox 3.6 or later, Apple Safari 6.2 or later, and Google Chrome. <b>Note:</b> The user interface is best viewed using Internet Explorer. Dashboard: The latest version of Adobe Flash Player (a browser based application runtime for viewing graphics) is required to view the dashboard.



## SaaS

For a SaaS (Fischer Identity as a Service® cloud) implementation, client organizations need to provide a gateway in each domain to be connected (except no gateway is required for applications that are connected via web services). Note that this gateway is also required in an on-premise implementation where Fischer Identity is in one domain and some systems to be connected are in another domain. The hardware listed above would be more than sufficient for the gateway.

### Global Identity Gateway UNIX Installation Prerequisites

<b>Operating system</b>	UNIX, Linux, Solaris 8 or later.
<b>Java support</b>	Sun Java Development Kit (JDK) 1.7.60 or later. A 64-bit version of Java is available on the IdM Suite Software folder\Additional Software\UNIX.
<b>Application server</b>	Apache Tomcat Web application server Version 7.0.54, which is available on the IdM Suite Software folder\Additional Software\UNIX. You must use same level (64-bit) for both Java and Apache Tomcat.
<b>Web Server</b>	Apache HTTPD

### Global Identity Gateway Windows Installation Prerequisites

<b>Software Requirements</b>	
<b>Operating system</b>	<b>One of these 64-bit version operating systems:</b> Windows Server 2008 R2, 2012, 2012 R2 or later.
<b>Java support</b>	Sun Java Development Kit (JDK) 1.7.60 or later. If not already installed, depending upon your operating system, use the 64-bit version from the IdM Suite Software folder\Additional Software\Windows\Java. Point the JAVA_HOME environment variable to the JDK installation directory, for example, C:\Program Files\Java\jdk1.7.0_60 for 64-bit.
<b>Application server</b>	Apache Tomcat Web application server Version 7.0.54 (included with the IdM Suite installation).
<b>Web Server</b>	Windows Internet Information Sharing (IIS)

## Communications & Access Testing Guide

---

The purpose of this guide is to help you troubleshoot the initial installation of the Fischer International Identity Suite. Please refer to the product installation guide for specifics about the installation process. This guide is to help you post-installation if you experience any communication-related issues while accessing the platform.

### Your Network Pre-Requisites

There are a few key items that need to begin immediately as we kickoff your project. First, let's make sure to get the VPN / remote access process started. Please communicate with your account manager or project manager to ensure that Fischer employees will have access to all they need access to in order to complete your deployment.

Fischer engineers will need access to the following devices within your network:

- The LDAP server designated for the Fischer product installation
- The RDBMS server designated for the Fischer product installation
- The Identity / Provisioning server where the Fischer software will install
- Any Global Identity Gateway servers that may be needed in your infrastructure

There are multiple ways our engineers typically gain access to these servers depending upon your network configuration and security policy, please let our team know what methods will be used. We can access via the following methods:

- Remote Desktop access to each of the servers listed above. RDP is not required to all servers but is required to the following:
  - The Identity / Provisioning server(s)
  - Any Global Identity Gateway server(s)
- Access to the Identity / Provisioning server(s) with application tools installed such as:
  - A database management application (SQL Manager for MSSQL, TOAD for Oracle, etc)
  - An LDAP browser to access the LDAP server

# Data Breach Response Policy

---

Prepared by: Fischer International Identity, LLC

Effective Date: 11/7/2015

## **Purpose**

This policy establishes how Fischer International Identity, LLC will respond in the event a data breach, and also outlines an action plan that will be used to investigate potential breaches and to mitigate damage if a breach occurs. This policy is in place to both minimize potential damages that could result from a data breach and to ensure that parties affected by a data breach are properly informed of how to protect themselves.

## **Scope**

This policy applies to all incidents where a breach of customer or employee personal identifying information is suspected or confirmed.

## **DEFINITIONS**

**Personal Identifying Information (PII)** – information that can be used to distinguish or trace an individual's identity. PII includes, but is not limited to, any of the following:

- Social Security numbers
- Credit card information (credit card numbers – whole or part; credit card expiration dates; cardholder names; cardholder addresses)
- Tax identification information numbers (Social Security numbers; business identification numbers; employer identification numbers)
- Biometric records (fingerprints; DNA; or retinal patterns and other measurements of physical characteristics for use in verifying the identity of individuals)
- Payroll information (paychecks; paystubs)
- Medical information for any employee or customer (doctor names and claims; insurance claims; prescriptions; any related personal medical information)
- Other personal information of a customer, employee or contractor (dates of birth; addresses; phone numbers; maiden names; names; customer numbers)

**Breach** – any situation where someone other than an authorized user accesses PII, for anything other than an authorized purpose.

## **POLICY GUIDELINES**

### **Upon Learning of a Breach**

A breach or a suspected breach of PII must be immediately investigated. Since all PII is of a highly confidential nature, only personnel necessary for the data breach investigation will be informed of the breach. The following information must be reported to appropriate management personnel:

- When (date and time) did the breach happen?
- How did the breach happen?
- What types of PII were obtained? (Detailed as possible: name; name and social security; Name, account and password; etc.)
- How many customers were affected?

Management will then make a record of events and people involved, as well as any discoveries made over the course of the investigation and determine whether or not a breach has occurred.

### **Perform a Risk Assessment**

Once a breach has been verified and contained, perform a risk assessment that rates the:

- Sensitivity of the PII Lost (Customer contact information alone may present much less of a threat than financial information)
- Amount of PII Lost and Number of Individuals Affected
- Likelihood PII Is Usable or May Cause Harm
- Likelihood the PII Was Intentionally Targeted (increases chance for fraudulent use)
- Strength and Effectiveness of Security Technologies Protecting PII (e.g. encrypted PII on a stolen laptop. Technically stolen PII but with a greatly decreased chance of access.)
- Ability of to Mitigate the Risk of Harm

All information collected during the risk assessment must then be compiled into one report and analyzed. The Risk Assessment must then be provided to appropriate personnel in charge of data breach response management.

### **Notifying Affected Parties**

Any information found in the initial risk assessment will be turned over to appropriate legal counsel for review to determine if, and to what extent, notification is required. Notification should occur in a manner that ensures the affected individuals will receive actual notice of the incident. Notification will be made in a timely manner, but will not occur until all facts are discovered as to thwart pre-mature notification that could exacerbate the initial incident with incomplete facts and public statements. In some cases, publicizing breaches prematurely can increase risk of a full breach, as opposed to a limited breach of specific information from specific people. In any cases notifications will be handled in accordance to the manner required and the magnitude of the breach.

In the case that notification must be made:

- Only the affected customer's [security principals] of Fischer International Identity, LLC will be informed of the breach. Notifying a broad base when it is not required could raise unnecessary concern in those who have not been affected.
- A physical copy will be mailed to the affected parties even if electronic methods are employed(e.g. phone, email or SMS).

The notification letter will include:

- A brief description of the incident. The nature of the breach and the approximate date it occurred.
- A description of the type(s) of PII that were involved in the breach. (The general types of PII, not an individual's specific information.)
- A detailed explanation pertaining to the breach investigation, mitigation and future prevention of breach incidents.
- Contact information for a representative who can answer additional questions.

### **Mitigating Risks**

Based off the findings of the risk assessment, a plan will be developed to mitigate the weakness that led to the breach. The exact course of action will be based on the type of PII that was involved in the data breach. The course of action will aim to minimize the effect of the initial breach and to prevent similar breaches from taking place.

- Affected customers will be notified as soon as possible so they can take their own steps to mitigate potential risk.

Fischer International Identity will also provide steps to mitigate risks that can be taken by affected individuals. The steps provided to affected individuals will depend on the nature of the data breach. If the breach has created a high risk for fraudulent use of financial information, customers may be advised to:


- Monitor their financial accounts and immediately report any suspicious or fraudulent activity.
- Contact the three major credit bureaus and place an initial fraud alert on their credit reports. This can be extremely helpful in situations where PII that can be used to open new accounts, such as social security numbers, has been taken.
- Avoid attempts from criminals that may see the breach

as an opportunity to pose as employees in an attempt to deceive affected individuals into divulging personal information.

- File a report with local police or in the community where the breach took place.
- Complete a Federal Trade Commission Threat Affidavit, available at [www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf](http://www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf). This form will allow the affected individual to notify their creditors that their identity has been compromised, and will minimize their liability for fraudulent use of their identity.

Instructions on what steps a customer can take to reduce their risk will be included in the notification letter. In addition to the information listed above, appropriate personnel, when possible, will provide additional information tailored to the individual breach.

Authorized By (Print): Daniel John Dagnall

Authorization Signature: 

Authorization Date: 6/15/2014

Attachment D

Answer to question T-DG-022 and T-DG-027



## Service Organization Control 2 Report

### Description of Rackspace US, Inc.'s Data center Services System relevant to Security and Availability

For the period October 1, 2014 through September 30, 2015

with the Independent Service Auditor's Report including Tests Performed and Results Thereof





**Rackspace US, Inc.  
Data center Services System**

**Table of Contents**

<b>Section Ia – Assertion of Rackspace US, Inc. ....</b>	<b>4</b>
<b>Section Ib – Assertion of DuPont Fabros Technology, Inc. (DFT) .....</b>	<b>6</b>
<b>Section Ic – Assertion of Equinix (UK) Limited (Equinix) .....</b>	<b>9</b>
<b>Section Id – Assertion of Digital Reality (DRT) .....</b>	<b>13</b>
<b>Section Ie – Assertion of Powerbase Data Centre Services HK facility (PCCW) .....</b>	<b>17</b>
<b>Section II – Independent Service Auditor’s Report .....</b>	<b>20</b>
<b>Section III – Description of Rackspace’s Data center Services System relevant to Security and Availability for the period October 1, 2014 through September 30, 2015 .....</b>	<b>25</b>
<i>Company Overview .....</i>	<i>25</i>
<i>Data center Services Overview .....</i>	<i>25</i>
<i>Role of Subservice Organizations .....</i>	<i>25</i>
<i>Relevant Aspects of the Control Environment, Risk Assessment, Monitoring, and Communication Processes .....</i>	<i>26</i>
Control Environment .....	26
Risk Assessment .....	28
Monitoring .....	29
Communication .....	29
<i>Description of Information Systems .....</i>	<i>30</i>
Organization and Management .....	30
Communication .....	32
Risk Management and Design and Implementation of Controls .....	34
Monitoring of Controls .....	35
Logical and Physical Access .....	35
Systems Operations .....	40
Change Management .....	41
Availability .....	42
<i>Trust Services Criteria and Related Controls .....</i>	<i>43</i>
<b>Section IV – Trust Services Security and Availability Principles, Criteria, Related Controls, and Tests of Controls .....</b>	<b>45</b>
<i>Testing Performed and Results of Tests of Entity-level Controls .....</i>	<i>45</i>
<i>Description of Information Systems .....</i>	<i>45</i>
Organization and Management .....	46
Communication .....	50
Risk Management and Design and Implementation of Controls .....	63
Monitoring of Controls .....	67
Logical and Physical Access .....	68
Systems Operations .....	96
Change Management .....	103
Availability .....	115
<b>Section V – Other Information Provided by Rackspace .....</b>	<b>121</b>

Section Ia - Assertion of Rackspace US, Inc.;  
Section Ib - Assertion of DuPont Fabros Technology, Inc.  
(DFT);  
Section Ic - Assertion of Equinix (UK) Limited (Equinix);  
Section Id - Assertion of Digital Realty (DRT) and  
Section Ie - Assertion of Powerbase Data Centre Services HK  
(PCCW)

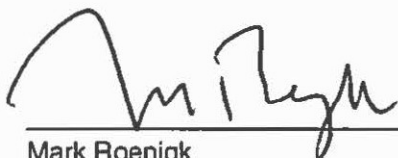
## Assertion of Rackspace US, Inc.

We have prepared the accompanying *Description of Rackspace US, Inc.'s Data center Services System relevant to Security and Availability for the period from October 1, 2014 through September 30, 2015* (Description) of Rackspace US, Inc. (Service Organization) based on the criteria in items (a)(i)-(ii) below, which are the criteria for a description of a service organization's system set forth in paragraph 1.26 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy* updated as of July 1, 2015 (the description criteria). The description is intended to provide users with information about the Data center Services system (System), particularly system controls, intended to meet the criteria for the security and availability principles set forth in the AICPA's TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

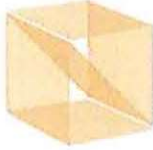
We confirm to the best of our knowledge and belief, that:

- a. the Description fairly presents the System throughout the period October 1, 2014 to September 30, 2015, based on the following description criteria:
  - i. the Description contains the following information:
    - (1) The types of services provided.
    - (2) The components of the system used to provide the services, which are the following:
      - Infrastructure. The physical structures, IT, and other hardware components of a system (for example, facilities, computers, equipment, mobile devices, and other telecommunication networks).
      - Software. The application programs and IT systems that support application programs (operating systems, middleware, and utilities).
      - People. The personnel involved in the governance, operation and use of a system (developers, operators, entity users, vendor personnel, and managers).
      - Procedures. The automated and manual procedures.
      - Data. Transaction streams, files, databases, tables, and output used or processed by the system.
    - (3) The boundaries or aspects of the system covered by the description.
    - (4) For information provided to, or received from, subservice organizations or other parties
      - (a) How such information is provided or received; the role of the subservice organization or other parties.
      - (b) The procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.
    - (5) The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:
      - (a) Complementary user-entity controls contemplated in the design of the Rackspace Data center Services system.

- (b) When the inclusive method is used to present a subservice organization, controls at the subservice organization.
  - (6) If the service organization presents the subservice organization using the carve-out method:
    - (a) The nature of the services provided by the subservice organization
    - (b) Each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria
  - (7) Any applicable trust services criteria that are not addressed by a control at the service organization or a subservice organization and the reasons therefore.
  - (8) In the case of a type 2 report, relevant details of changes to the service organization's system during the period covered by the Description.
- ii. the Description does not omit or distort information relevant to the service organization's system while acknowledging that the Description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.
- b. the controls stated in the Description were suitably designed to provide reasonable assurance that the applicable trust services criteria were met if the controls operated as described and if user entities applied the complementary user entity controls contemplated in the design of Rackspace's controls throughout the period October 1, 2014 to September 30, 2015.
- c. the Rackspace controls stated in the description operated effectively throughout the specified period to meet the applicable trust services criteria.



Mark Roenigk  
Chief Operating Officer



DuPont Fabros Technology

1212 New York Ave, NW  
Suite 900  
Washington, DC 20005

P (202) 728-0044  
F (202) 728-0220  
www.dft.com

## Assertion of DuPont Fabros Technology, Inc. (DFT)

We have read the portion of the accompanying *Description of Rackspace US, Inc.'s Data center Services System relevant to Security and Availability for the period October 1, 2014 through September 30, 2015* (Description) relevant to Corporate Security and Data center Access and Environmental Controls provided by DuPont Fabros Technology, Inc. to Rackspace US, Inc. (DuPont Fabros Technology, Inc. services) based on the criteria in items (a)(i)-(ii) below, which are the criteria for a description of a service organization's system set forth in paragraph 1.26 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* (the description criteria). The Description was prepared by Rackspace US, Inc. to provide users with information about Rackspace's Data center Services system (System), particularly system controls, intended to meet the criteria for the security and availability principles set forth in the AICPA's TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality and Privacy* (applicable trust services criteria). The management of DuPont Fabros Technology, Inc. confirms, to the best of its knowledge and belief, that:

- a. the portion of the Description relevant to the services fairly presents the services provided by DuPont Fabros Technology, Inc. to Rackspace US, Inc. throughout the period October 1, 2014 to September 30, 2015 based on the following criteria:
  - i. the Description contains the following information:
    - (1) The types of services provided.
    - (2) The components of the system used to provide the services, which are the following:
      - Infrastructure. The physical and hardware components of the system (facilities, equipment, and networks).
      - Software. The programs and operating software of the system (systems, applications, and utilities).
      - People. The personnel involved in the operation and use of the system (developers, operators, users, and managers).
      - Procedures. The automated and manual procedures involved in the operation of the system.
      - Data. The information used and supported by the system (transaction streams, files, databases, and tables).

- (3) The boundaries or aspects of the system covered by the Description.
  - (4) How the system captures and addresses significant events and conditions.
  - (5) The process used to prepare and deliver reports and other information to user entities and other parties.
  - (6) If information is provided to, or received from, subservice organizations or other parties, how much information is provided or received; the role of the subservice organization and other parties; and the procedures performed to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.
  - (7) For each principle being reported on, the applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user-entity controls contemplated in the design of the service organization's system.
  - (8) For subservice organizations presented using the carve-out method, the nature of the services provided by the subservice organization; each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria.
  - (9) Any applicable trust services criteria that are not addressed by a control at the service organization or a subservice organization and the reasons therefore.
  - (10) Other aspects of the service organization's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria.
  - (11) Relevant details of changes to the service organization's system during the period covered by the Description.
- ii. the Description does not omit or distort information relevant to the service organization's system, while acknowledging that the portion of the Description relevant to the DuPont Fabros Technology, Inc. services provided by DuPont Fabros Technology, Inc. is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.
- b. the controls performed by DuPont Fabros Technology, Inc. stated in the Description if operating effectively, were suitably designed by Rackspace US, Inc. throughout the specified period to meet the applicable trust services criteria.
  - c. the Dupont Fabros Technology, Inc. controls stated in the Description operated effectively throughout the specified period to meet the applicable trust services criteria.

A handwritten signature in black ink, appearing to read 'Carlos A. Colmenero', written in a cursive style. The signature is positioned above a thin horizontal line.

Carlos A. Colmenero  
Senior Property Manager  
DuPont Fabros Technology, Inc.

## Equinix (UK) Limited's Management Assertion

We have read the portions of the accompanying *Description of Rackspace US, Inc.'s Data center Services System relevant to Security and Availability for the period from October 1, 2014 through September 30, 2015* (Description) relevant to Corporate Security and Data center Access and Environmental Controls provided by Equinix (UK) Limited (Equinix) to Rackspace US, Inc. (Services) which is attached hereto, based on the criteria in items (a)(i)-(ii) below, which are the criteria for a description of a service organization's system set forth in paragraph 1.34 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy* (the description criteria), and prepared by Rackspace US, Inc. to provide users with information about Rackspace's Data center Services system (System), particularly system controls, intended to meet the criteria for the security and availability principles set forth in the AICPA's TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

The management of Equinix confirms, to the best of its knowledge and belief, that:

- a. the portion of the Description relevant to the Services fairly presents the services provided by Equinix to Rackspace US, Inc. throughout the period October 1, 2014 to September 30, 2015, based on the following description criteria:
  - i. the Description contains the following information:
    - (1) The types of Services provided
    - (2) The components of the system used to provide the Services, which are the following:
      - Infrastructure. The physical and hardware components of a system (facilities, equipment, and networks).
      - Software. The programs and operating software of a system (systems, applications, and utilities).
      - People. The personnel involved in the operation and use of a system (developers, operators, users, and managers).
      - Procedures. The automated and manual procedures involved in the operation of a system.
      - Data. The information used and supported by a system (transaction streams, files, databases, and tables).
    - (3) The boundaries or aspects of the system covered by the Description.
    - (4) How the system captures and addresses significant events and conditions.



- 
- (5) The process used to prepare and deliver reports and other information to user entities or other parties.
  - (6) If information is provided to, or received from, subservice organizations or other parties, how such information is provided or received; the role of the subservice organization or other parties; and the procedures performed to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.
  - (7) For each principle being reported on, the applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user-entity controls contemplated in the design of the service organization's system.
  - (8) For subservice organizations presented using the carve-out method, the nature of the services provided by the subservice organization; each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria.
  - (9) Any applicable trust services criteria that are not addressed by a control at the service organization or a subservice organization and the reasons therefore.
  - (10) Other aspects of the service organization's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria.
  - (11) Relevant details of changes to the service organization's system during the period covered by the Description.
- ii. the Description does not omit or distort information relevant to Equinix's Services while acknowledging that the portion of the Description relevant to the Equinix Services is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of Equinix's Services that each individual user may consider important to his or her own particular needs.
- b. the controls performed by Equinix stated in the Description were suitably designed throughout the specified period to meet the applicable trust services criteria.
  - c. the Equinix controls stated in the Description operated effectively throughout the specified period to meet the applicable trust services criteria.

Very truly yours,



Russell Poole  
Managing Director, Equinix (UK) Limited



15 JAN 2016



## Assertion of Equinix Australia Pty Limited (Equinix)

We have read the portions of the accompanying *Description of Rackspace US, Inc.'s Data center Services System relevant to Security and Availability for the period from October 1, 2014 through September 30, 2015* (Description) relevant to Corporate Security and Data center Access and Environmental Controls provided by Equinix to Rackspace US, Inc. (Services) which is attached hereto, based on the criteria in items (a)(i)-(ii) below, which are the criteria for a description of a service organization's system set forth in paragraph 1.34 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy* (the description criteria), and prepared by Rackspace US, Inc. to provide users with information about Rackspace's Data center Services system (System), particularly system controls, intended to meet the criteria for the security and availability principles set forth in the AICPA's TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

We confirm, to the best of our knowledge and belief, that:

- a. the portion of the Description relevant to the Services fairly presents the services provided by Equinix to Rackspace US, Inc. throughout the period October 1, 2014 to September 30, 2015, based on the following description criteria:
  - i. the Description contains the following information:
    - (1) The types of Services provided
    - (2) The components of the system used to provide the Services, which are the following:
      - Infrastructure. The physical and hardware components of a system (facilities, equipment, and networks).
      - Software. The programs and operating software of a system (systems, applications, and utilities).
      - People. The personnel involved in the operation and use of a system (developers, operators, users, and managers).
      - Procedures. The automated and manual procedures involved in the operation of a system.
      - Data. The information used and supported by a system (transaction streams, files, databases, and tables).
    - (3) The boundaries or aspects of the system covered by the Description.
    - (4) How the system captures and addresses significant events and conditions.
    - (5) The process used to prepare and deliver reports and other information to user entities or other parties.
    - (6) If information is provided to, or received from, subservice organizations or other

CONFIDENTIAL – PRIVILEGED AND CONFIDENTIAL

All information transmitted hereby is intended only for the use of the addressee(s) named above. If the reader of the message is not the intended recipient or employee or agent responsible for delivering the message to the intended recipient(s), please note that any distribution or copying of this communication is strictly forbidden. Anyone who receives this communication in error should notify us immediately by telephone and return the original message to us at the above address via the appropriate Postal service.

parties, how such information is provided or received; the role of the subservice organization or other parties; and the procedures performed to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

- (7) For each principle being reported on, the applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user-entity controls contemplated in the design of the service organization's system.
  - (8) For subservice organizations presented using the carve-out method, the nature of the services provided by the subservice organization; each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria.
  - (9) Any applicable trust services criteria that are not addressed by a control at the service organization or a subservice organization and the reasons therefore.
  - (10) Other aspects of the service organization's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria.
  - (11) Relevant details of changes to the service organization's system during the period covered by the Description.
- ii. the Description does not omit or distort information relevant to Equinix's Services while acknowledging that the portion of the Description relevant to the Equinix Services is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of Equinix's Services that each individual user may consider important to his or her own particular needs.
- b. the controls performed by Equinix stated in the Description were suitably designed throughout the specified period to meet the applicable trust services criteria.
  - c. the Equinix controls stated in the Description operated effectively throughout the specified period to meet the applicable trust services criteria.

Very truly yours,



---

Jeremy Deutsch  
Managing Director, Equinix Australia Pty Limited

CONFIDENTIAL – PRIVILEGED AND CONFIDENTIAL

All information transmitted hereby is intended only for the use of the addressee(s) named above. If the reader of the message is not the intended recipient or employee or agent responsible for delivering the message to the intended recipient(s), please note that any distribution or copying of this communication is strictly forbidden. Anyone who receives this communication in error should notify us immediately by telephone and return the original message to us at the above address via the appropriate Postal service.

## Assertion of Digital Realty (DRT)

Re: Lease dated May 20, 2011 (as amended from time to time, the “1232 Alma Lease”), between Rackspace US, Inc. (“Rackspace US”) and Collins Technology Park Partners, LLC (“CTPP”), covering certain premises (the “1232 Alma Premises”) more particularly described in the 1232 Alma Lease at that certain building located at 1232 Alma Road, Richardson, TX 75081 (the “1232 Alma Building”); Lease dated December 29, 2011 (as amended from time to time, the “1215 Integrity Lease”), between Rackspace US and CTPP, covering certain premises (the “1215 Integrity Premises”) more particularly described in the 1215 Integrity Lease at that certain building located at 1215 Integrity Drive, Richardson, TX 75081 (the “1215 Integrity Building”); Agreement for Lease dated January 11, 2013, Turn Key Data Centre Lease date April 16, 2015, and Turn Key Data Centre Lease dated August 20, 2015 (each as amended from time to time, the “Crawley Leases”) between Rackspace Limited (“Rackspace Limited”) and Digital Crawley 1 Sarl (“DC1S”) covering certain premises (the “Crawley Premises”) more particularly described in the Crawley Leases at that certain building located at Principal Park, Manor Royal, Crawley, RH10 9QJ, England (the “Crawley Building”); and Lease dated June 30, 2012 (as amended from time to time, the “1-23 Templar Lease” and together with the 1232 Alma Lease and the 1215 Integrity Lease, the “Leases”), between Rackspace Hosting Pty Limited (“Rackspace Hosting” and, collectively with Rackspace US and Rackspace Limited, “Tenant”) and Digital Realty Datafirm, LLC (“DRD” and, collectively with CTPP and DC1S, “Landlord”), covering certain premises (the “1-23 Templar Premises” and together with the 1232 Alma Premises, the Crawley Premises and the 1215 Integrity Premises, the “Premises”) more particularly described in the 1-23 Templar Lease at that certain building located at 1-23 Templar Road, Erskine Park, New South Wales 2759, Australia (the “1-23 Templar Building” and, together with the 1232 Alma Building, the Crawley Building and the 1215 Integrity Building, the “Buildings”).

Tenant has prepared, and Landlord has read, the portions of the accompanying Description of Rackspace US, Inc.’s Data center Services System relevant to Security and Availability for the period October 1, 2014 through September 30, 2015 (Description) relevant to Corporate Security and Data center Access and Environmental Controls provided by Landlord to Tenant (Digital Realty services) based on the criteria in items (a)(i)-(ii) below, which are the criteria for a description of a service organization’s system set forth in paragraph 1.26 of the AICPA Guide Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (the description criteria). The Description was prepared by Tenant to provide users with information about Tenant’s Data center Services system (System), particularly system controls, intended to meet the criteria for the security and availability principles set forth in the AICPA’s TSP section 100, Trust Services Principles, Criteria, and

Illustrations for Security, Availability, Processing Integrity, Confidentiality and Privacy (applicable trust services criteria). Landlord confirms, to the best of its knowledge and belief, that:

- a. the portion of the Description relevant to the Digital Realty services fairly presents the services provided by Landlord to Tenant throughout the period October 1, 2014 to September 30, 2015 based on the following criteria, as applicable:
  - i. the Description contains the following information:
    - (1) The types of services provided.
    - (2) The components of the system used to provide the services, which are the following:
      - Infrastructure. The physical and hardware components of the system (facilities, equipment, and networks).
      - Software. The programs and operating software of the system (systems, applications, and utilities).
      - People. The personnel involved in the operation and use of the system (developers, operators, users, and managers).
      - Procedures. The automated and manual procedures involved in the operation of the system.
      - Data. The information used and supported by the system (transaction streams, files, databases, and tables).
    - (3) The boundaries or aspects of the system covered by the Description.
    - (4) How the system captures and addresses significant events and conditions.
    - (5) The process used to prepare and deliver reports and other information to Tenant and other parties.
    - (6) If information is provided to, or received from, subservice organizations or other parties, how such information is provided or received; the role of the subservice organization and other parties; and the procedures performed to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.
    - (7) For each principle being reported on, the applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user-entity controls contemplated in the design of the service organization's system.
    - (8) For subservice organizations presented using the carve-out method, the nature of the services provided by the subservice organization; each of the applicable trust services criteria that are intended to be met by controls at the subservice

organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria.

- (9) Any applicable trust services criteria that are not addressed by a control at the service organization or a subservice organization and the reasons therefor.
  - (10) Other aspects of the service organization's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria.
  - (11) Relevant details of changes to the service organization's system during the period covered by the Description.
- ii. the Description does not omit or distort information relevant to the service organization's system, while acknowledging that the portion of the Description relevant to the Digital Realty services provided by Landlord is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.
- b. Landlord's Controls stated in the Description were suitably designed throughout the specified period to meet the applicable trust services criteria.
  - c. Landlord's Controls stated in the Description operated effectively throughout the specified period to meet the applicable trust services criteria.

The controls that Landlord executes as part of the Digital Realty services that support the control objectives for Tenant's physical security and environmental controls described above are as follows (collectively, Landlord's Controls): Key card access restrictions and building lobby security limit access to facilities in addition to receptionist and/or Tenant employees.

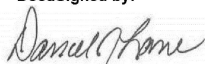
The term "to the best of Landlord's knowledge and belief," and similar phrases utilized herein shall mean and refer to the actual current knowledge, as of the date of this assertion, of Danny Lane (the foregoing individual being someone who would have direct and specific knowledge regarding the applicable Building, but who shall not have the duty of additional investigation in connection with this assertion).

While Landlord is making certain assertions and representations related to Landlord's Controls that were in effect during the period October 1, 2014 to September 30, 2015, (a) nothing contained in this assertion shall be deemed to create a requirement that such controls remain in effect at any point in the future, (b) nothing contained in this assertion shall be deemed to imply



that Landlord was required (except for the extent expressly required under the terms of the Leases) to have any of such controls in effect at any point during the period October 1, 2014 to September 30, 2015, and (c) none of such representations or assertions shall be deemed to modify or append any of Landlord's requirements and/or obligations under the Leases (which may, or may not, include the requirement of Landlord to establish and/or maintain any or all of Landlord's Controls in effect at the Buildings).

This assertion is provided to Ernst & Young LLP and is solely for Ernst & Young LLP, Tenant and Tenant's user entities in connection with Ernst & Young LLP's engagement to report on the Description throughout the period October 1, 2014 to September 30, 2015 at the Buildings. The assertion may not be used by Ernst & Young LLP, Tenant and Tenant's user entities for any other purposes, or furnished to, assigned to, quoted to, or relied upon by any other person or entity for any purposes without Landlord's prior written consent.

DocuSigned by:  
  
08B0F24D970C433...

---

Danny Lane

Vice President, Property Operations



## Assertion of PCCW Powerb@se Data Center Services (HK) Limited (PCCW)

We have read the portions of the accompanying *Description of Rackspace US, Inc.'s Data center Services System relevant to Security and Availability for the period October 1, 2014 through September 30, 2015* (Description) relevant to Corporate Security and Data center Access and Environmental Controls provided by PCCW to Rackspace US, Inc. (PCCW services) based on the criteria in items (a)(i)-(ii) below, which are the criteria for a description of a service organization's system set forth in paragraph 1.26 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* (the description criteria). The Description was prepared by Rackspace US, Inc. to provide users with information about Rackspace's Data center Services system (System), particularly system controls, intended to meet the criteria for the security and availability principles set forth in the AICPA's TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality and Privacy* (applicable trust services criteria). The management of PCCW confirms, to the best of its knowledge and belief, that:

- a. the portion of the Description relevant to the services fairly presents the services provided by PCCW to Rackspace US, Inc. throughout the period October 1, 2014 to September 30, 2015 based on the following criteria:
  - i. the Description contains the following information:
    - (1) The types of services provided.
    - (2) The components of the system used to provide the services, which are the following:
      - Infrastructure. The physical and hardware components of the system (facilities, equipment, and networks).
      - Software. The programs and operating software of the system (systems, applications, and utilities).
      - People. The personnel involved in the operation and use of the system (developers, operators, users, and managers).
      - Procedures. The automated and manual procedures involved in the operation of the system.
      - Data. The information used and supported by the system (transaction streams, files, databases, and tables).
    - (3) The boundaries or aspects of the system covered by the Description.
    - (4) How the system captures and addresses significant events and conditions.
    - (5) The process used to prepare and deliver reports and other information to user entities and other parties.
    - (6) If information is provided to, or received from, subservice organizations or other parties, how much information is provided or received; the role of the subservice organization and other parties; and the procedures performed to





determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

- (7) For each principle being reported on, the applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user-entity controls contemplated in the design of the service organization's system.
  - (8) For subservice organizations presented using the carve-out method, the nature of the services provided by the subservice organization; each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria.
  - (9) Any applicable trust services criteria that are not addressed by a control at the service organization or a subservice organization and the reasons therefore.
  - (10) Other aspects of the service organization's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria.
  - (11) Relevant details of changes to the service organization's system during the period covered by the Description.
- ii. the Description does not omit or distort information relevant to the service organization's system, while acknowledging that the portion of the Description relevant to the PCCW services provided by PCCW is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.
- b. the controls performed by PCCW stated in the Description if operating effectively, were suitably designed by Rackspace US, Inc. throughout the specified period to meet the applicable trust services criteria.
  - c. the PCCW controls stated in the Description operated effectively throughout the specified period to meet the applicable trust services criteria.

A handwritten signature in black ink, appearing to read "John Yow", written over a horizontal line.

John Yow  
Vice President  
PCCW Powerb@se Data Center Services (HK) Limited

## Section II – Independent Service Auditor's Report



Ernst & Young LLP  
Frost Bank Tower  
Suite 1700  
100 West Houston Street  
San Antonio, TX 78205

Tel: +1 210 228 9696  
Fax: +1 210 242 7252  
ey.com

## Section II – Independent Service Auditor’s Report

The Board of Directors  
Rackspace US, Inc.

### Scope

We have examined Rackspace US, Inc.’s (Rackspace) accompanying *Description of Rackspace’s Data center Services System relevant to Security and Availability for the period October 1, 2014 through September 30, 2015* (Description) of its hosted services and DFT’s, Equinix’s, DRT’s and PCCW’s descriptions of relevant aspects of their physical security and Data center environmental safeguards services throughout the period October 1, 2014 through September 30, 2015 based on the criteria set forth in paragraph 1.26 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy* updated as of July 1, 2015 (the description criteria) and the suitability of the design and operating effectiveness of Rackspace’s, DFT’s, Equinix’s, DRT’s and PCCW’s controls described therein to meet the criteria for the security and availability principles set forth in the AICPA’s TSP section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria) throughout the period October 1, 2014 to September 30, 2015.

DFT, Equinix, DRT and PCCW are independent service organizations that provide physical security and Data center environmental safeguards services to Rackspace. Rackspace’s Description includes a description of DFT’s, Equinix’s, DRT’s and PCCW’s services used by Rackspace, as well as relevant controls of DFT, Equinix, DRT and PCCW.

The information in the accompanying *Other information provided by Rackspace US, Inc.* is presented by management of Rackspace to provide additional information and is not part of Rackspace’s Description. Such information has not been subjected to the procedures applied in our examination and, accordingly we express no opinion on it.

### Rackspace’s responsibilities

Rackspace has provided the accompanying assertion titled *Assertion of Rackspace US, Inc.* (Assertion) about the fairness of the presentation of the Description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria. Rackspace is responsible for (1) preparing the Description and Assertion, (2) the completeness, accuracy, and method of presentation of the Description and Assertion, (3) providing the services covered by the Description; (4) specifying the controls that meet the applicable trust services criteria and stating them in the Description; and (5) designing, implementing, and documenting controls to meet the applicable trust services criteria.

### DFT’s responsibilities

DFT has provided its accompanying assertion titled *Assertion of DuPont Fabros Technology, Inc.* (DFT Assertion) about the fairness of the presentation of certain controls in the Description (DFT controls) and suitability of the design and operating effectiveness of the DFT

controls to meet the related applicable trust services criteria. DFT is responsible for preparing the DFT Assertion, including the completeness, accuracy and method of presentation of the DFT Assertion.

DFT is also responsible for providing certain services covered by the Description, specifying the DFT controls that meet the applicable trust services criteria and stating them in the Description; and implementing and documenting controls to meet the applicable trust services criteria.

#### Equinix's responsibilities

Equinix has provided its accompanying assertion titled *Assertion of Equinix (UK) Limited* (Equinix Assertion) about the fairness of the presentation of certain controls in the Description (Equinix controls) and suitability of the design and operating effectiveness of the Equinix controls to meet the related applicable trust services criteria. Equinix is responsible for preparing the Equinix Assertion, including the completeness, accuracy and method of presentation of the Equinix Assertion.

Equinix is also responsible for providing certain services covered by the Description, specifying the Equinix controls that meet the applicable trust services criteria and stating them in the Description; and implementing and documenting controls to meet the applicable trust services criteria.

#### DRT's responsibilities

DRT has provided its accompanying assertion titled *Assertion of Digital Reality (DRT)* (DRT Assertion) about the fairness of the presentation of certain controls in the Description (DRT controls) and suitability of the design and operating effectiveness of the DRT controls to meet the related applicable trust services criteria. DRT is responsible for preparing the DRT Assertion, including the completeness, accuracy and method of presentation of the DRT Assertion.

DRT is also responsible for providing certain services covered by the Description, specifying the DRT controls that meet the applicable trust services criteria and stating them in the Description; and implementing and documenting controls to meet the applicable trust services criteria.

#### PCCW's responsibilities

PCCW has provided its accompanying assertion titled *Assertion of Powerbase Data Centre Services HK (PCCW)* (PCCW Assertion) about the fairness of the presentation of certain controls in the Description (PCCW controls) and suitability of the design and operating effectiveness of the PCCW controls to meet the related applicable trust services criteria. PCCW is responsible for preparing the PCCW Assertion, including the completeness, accuracy and method of presentation of the PCCW Assertion.

PCCW is also responsible for providing certain services covered by the Description, specifying the PCCW controls that meet the applicable trust services criteria and stating them in the Description; and implementing and documenting controls to meet the applicable trust services criteria.

#### Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the Description based on the description criteria and on the suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the Description is fairly presented based on the description criteria, and (2) the controls described therein were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period October 1, 2014 through September 30, 2015.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service and subservice organizations' controls involves performing procedures to obtain evidence about the fairness of the presentation of the Description based on the description criteria and the suitability of the design and operating effectiveness of those controls to meet the applicable trust services criteria. Our procedures included assessing the risks that the Description is not fairly presented and that the controls were not suitably designed or operating effectively. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the applicable trust services criteria were met. Our examination also included evaluating the overall presentation of the Description. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

#### Inherent limitations

The Description is prepared to meet the common needs of a broad range of users, and may not, therefore, include every aspect of the system that each individual user may consider important to its own particular needs. Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria, is subject to the risk that the system may change or that controls at a service organization may become ineffective or fail.

Opinion

In our opinion, in all material respects, based on the description criteria and the applicable trust services criteria:

- a. The Description fairly presents Rackspace's Data center Services System and DFT's, Equinix's, DRT's and PCCW's physical security and Data center environmental safeguards services used by Rackspace to host customer servers for security and availability that was designed and implemented throughout the period October 1, 2014 through September 30, 2015.
- b. The controls of Rackspace, DFT, Equinix, DRT and PCCW stated in the Description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period October 1, 2014 through September 30, 2015.
- c. The controls tested operated effectively to provide reasonable assurance that the applicable trust services criteria were met throughout the period October 1, 2014 through September 30, 2015.

Description of tests of controls

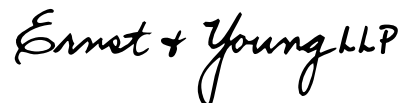
The specific controls tested and the nature, timing and results of those tests are listed in the accompanying *Trust Services Security and Availability Principles, Criteria, Related Controls, and Tests of Controls* (Description of Tests and Results).

Restricted use

This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of Rackspace, user entities of Rackspace's Data centers Services System, and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- ▶ The nature of the service provided by the service organization
- ▶ How the service organization's system interacts with user entities, subservice organizations, and other parties
- ▶ Internal control and its limitations
- ▶ The applicable trust services criteria
- ▶ The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.



January 14, 2016

**Section III – Description of Rackspace’s Data center Services  
System relevant to Security and Availability for the period  
October 1, 2014 through September 30, 2015**

## **Section III – Description of Rackspace’s Data center Services System relevant to Security and Availability for the period October 1, 2014 through September 30, 2015**

### ***Company Overview***

Rackspace US, Inc. (Rackspace, or Company) began operations in December 1998 to provide managed web hosting services to small to medium sized businesses. Today, Rackspace services over 300,000 customers, including many Fortune 500 companies, in thirteen Data centers worldwide. Currently, Rackspace employs over 6,000 people (Rackers) around the world.

Rackspace integrates the industry's leading technologies and practices for each customer's specific need and delivers it as a service via the Company's commitment to Fanatical Support®.

### ***Data center Services Overview***

Rackspace services a broad range of customers with diverse hosting needs and requirements. Rackspace has Dedicated, Cloud and Hybrid Hosting segments to support their clients. Rackspace Hybrid Hosting offers a combination of hosting services that enables customers to use managed hosting and cloud services under one account. Cloud Hosting is the newest division of Rackspace that serves clients scalable IT-enabled capabilities using Internet technologies. Rackspace has a third segment, called Managed Colocation, which serves clients that have significant in-house expertise and only require support around physical infrastructure.

This report is limited to the Data center Services across various office locations (San Antonio, TX and Hayes, UK), Rackspace owned Data center facilities (DFW1, LON3), and leased Data center facilities (ORD1, IAD2, IAD3, DFW2, DFW3, LON1, LON3 Data Hall 4, LON5, HKG1, SYD2, and SYD4).

### ***Role of Subservice Organizations***

The role of subservice organizations used by Rackspace is to provide physical and environmental security at Data centers not directly owned by Rackspace. Since these locations are not owned by Rackspace, reliance on subservice organizations' controls is needed to complete audits and examinations that include security and environmental controls. Controls at Rackspace subservice organizations are more stringent than or equal to the controls found in Rackspace-owned Data centers.



## ***Relevant Aspects of the Control Environment, Risk Assessment, Monitoring, and Communication Processes***

This section provides information about four interrelated components of internal control at Rackspace:

### **Control Environment**

A Company's internal control environment reflects the overall attitude, awareness and actions of management and the board of directors concerning the importance of controls and the emphasis given to controls in the Company's policies, procedures, methods, and organizational structure. The following is a description of the control environment as it pertains to Rackspace's delivery of IT hosting services.

#### **Business Segmentation**

Rackspace is internally organized into business units or "segments." They include: Dedicated Hosting (Managed Hosting), Managed Colocation, Cloud (refer to Section V for a list of Cloud products and services), and E-mail and Apps. Eight global functions support these segments:

- Engineering
- Accounting & Finance
- Legal
- Employee Services
- Sales & Marketing
- Information Technology
- Corporate Development/Strategy
- Global Enterprise Security

These global functions have been established to provide capabilities to complement the segments, and to realize economies of scale and quality control. Each segment is led by a segment leader. The leaders of the various global functions, the segment leaders, and Corporate officers make up the Rackspace Leadership Team.

#### **Internal Controls**

Rackspace management is responsible for directing and controlling operations and for establishing, communicating and monitoring policies, standards and procedures. Rackspace achieves operational and strategic compliance to the Company's overall objectives through proper preparation, planning, execution and governance.

Importance is placed on maintaining sound and effective internal controls and the integrity and ethical values of all Rackspace personnel. Rackspace takes actions to address risks to the achievement of these objectives by making available the organizational values and behavioral standards in the Rackspace Employee Handbook.

Rackspace promotes a culture based on core values defined by management and carried out by all Rackspace employees. These core values compliment the Company's ethical values, integrity model, professional conduct standards, and employee development pathways. The sum of these values and behaviors form Rackspace's unique environment by influencing the control consciousness of its employees.

### **Commitment to Competence**

The competence of employees is a key element of the control environment. The Human Resources Team performs a review of key talent, by individual and role, to ensure that critical talent is retained. This serves to ensure that the organizational structure is aligned in a way that will support the achievement of the Company's objectives and strategies. Rackspace employs staff with high levels of technical, risk and business knowledge in order to ensure proper handling of critical issues. Rackspace is committed to the development of its employees.

This commitment to competence is expressed in the Company's personnel policies and related human resource programs. Specific indicators of the commitment to personnel development include recruiting and hiring policies, investment in training and development, and performance monitoring. Rackspace's commitment to competence begins with recruiting, which is the joint responsibility of the Employee Services Department and business unit or department managers. Hiring decisions are based on various factors, including educational background, prior relevant experience, past accomplishments, and indication of integrity and ethical behavior.

Rackspace's commitment to the training and development of its employees is demonstrated by the creation of a dedicated training organization called Rackspace University. Rackspace provides and encourages training to its employees to assure that appropriate knowledge and skills are maintained. The training and development path is co-managed by each employee and their manager. All training is coordinated through Rackspace University. The process entails the development of specific, quantifiable objectives for the coming performance year, periodic discussions of progress in achieving those objectives, and a quarterly formal review of the employee's overall performance in the current position. It also fosters career development discussions to help prepare the individual for advancement.

Each department within Rackspace is given a dedicated training budget for each of the members of the department. This budget is renewed annually. The Rackspace Finance Department manages the training budget for the Company as a whole and individual managers are responsible for their team budgets. Managers work with each team member to research and suggest training that is beneficial for the Racker in the function they perform and to foster professional growth within the Company.

Rackspace technicians are staffed on a 24/7 basis to offer assistance with customer inquiries. Additionally, Rackspace support teams and Data center operations teams with technicians certified in various areas of expertise. Certifications held by Rackspace technicians include, but are not limited to:

- Microsoft Certified Systems Engineer
- Microsoft Certified Professional

- Microsoft Certified Trainer
- Red Hat Certified Engineer
- Certified Information Systems Security Professional
- Certified Information Security Manager
- Certified Fraud Examiner
- Certified Protection Professional
- Cisco Certified Internetwork Expert
- Brocade Certified Fabric Professional
- Dell Certified Systems Expert
- Legato Certified Networker Administrator
- VMware Certified Engineers

Rackspace is also a Microsoft Gold Certified Partner and maintains a Microsoft Premier Services Agreement to provide vendor assistance and escalation of critical issues. Rackspace is a Cisco Service Provider Partner and the Company maintains a Cisco support and maintenance contract, which includes software upgrades, hardware support and replacement, and support from the Cisco Technical Assistance Center (TAC).

## **Risk Assessment**

Information Security Risk Assessments are completed by the Global Enterprise Security team (GES) and require sign-off from leadership around the Company. Leadership then makes decisions based on the evolving risk at the Company. These decisions are expressed through the implementation of global strategies and process changes.

The Rackspace risk assessment process includes the identification, analysis, and management of risks that could impact the Company's network infrastructure, application development, data management, and business operations. Rackspace recognizes its risk management methodology and processes as critical components of its operations to verify that customer assets are properly maintained. Rackspace incorporates risk management throughout its processes at both the corporate and segment levels.

Rackspace manages risks on an ongoing basis through a formal risk assessment process. The Global Enterprise Security Risk Management team identifies, assesses, prioritizes, and evaluates risk based on the Security Risk Management Plan. In addition to the formal risk assessment process, managers discuss and resolve issues as they arise within their areas. Also, managers monitor and adjust the control processes for which they are responsible on an as-needed basis.

This process is performed both informally and formally through regularly scheduled meetings and by the formation of a cross-functional team to manage Global Enterprise Security initiatives and projects. The ESWG (Enterprise Security Working Group) brings together members from various business units to discuss security risks, priorities and challenges. Additionally, the Risk Management team presents the Company's top ten risks to the Internal Audit department and the Audit Committee for their review and consideration while developing their risk based audit plan.

Rackspace has an Enterprise strategic plan that is presented to the Board of Directors on a quarterly basis. This strategic plan is then separated into specific segment plans that are designed to operationalize what is expected of the segments in order to support Rackspace's overall objectives. Rackspace in-house legal counsel reviews contracts and amendments with vendors and customers. Finally, monitoring of performance against existing contracts with vendors and customers is a critical function performed by all of Rackspace's segments.

## **Monitoring**

Monitoring is a critical aspect in evaluating whether controls are operating as intended and whether they are updated as necessary to reflect changes in the processes. Management and supervisory personnel are responsible for monitoring the quality of internal control performance as a routine part of their activities.

Rackspace monitors compliance with leading security practices and internal security policies through the routine audit and assessment of its systems and processes. Assessments are performed following applicable industry standards and third party audit firms are engaged in the assessment when appropriate. To complement these measures, exceptions to procedural problems are logged, reported, and tracked until resolved.

Rackspace creates a series of management reports that detail efforts to provide a robust, scalable, and secure infrastructure for client organizations. The Data center personnel continuously monitor processing capacity while Data center power utilization metrics are distributed to Rackspace leadership on a monthly basis.

Performance metric reports include data on actual system availability compared with established service level goals and standards. Management reviews performance metric reports and take action when appropriate.

## **Communication**

Rackspace management realizes that an effective communication with personnel is vital in order to align Rackspace business strategies and goals with operating performance. The Company maintains an organizational structure to properly note lines of reporting within each department and job responsibility, and organizational values and behavioral standards are communicated to personnel via the Rackspace's Intranet and the Rackspace Employee Handbook. The Employee Handbook is signed by new hires on their hiring date and a Code of Conduct Agreement is distributed to employees upon hiring.

Rackspace supports customer satisfaction by monitoring customer communication and issue resolution. Customer communication is handled through the Rackspace customer portal and through the Company's website which hosts and communicates our commitment availability as stated in the Service Level Agreement and our commitment to security included in the General Terms and Conditions.

Rackspace personnel can access key performance metrics using the Rackspace Data Warehouse on a real time basis. Members of management from across several functional divisions participate in weekly meetings to discuss the status of service delivery or other matters of interest and concern. Issues or suggestions identified by personnel are readily brought to the attention of management to be addressed and resolved.

In addition, a monthly Directors and Officers report is provided to Rackspace management summarizing the performance statistics of the various segments within the Company. This report includes, but is not limited to, key financial data, employee headcount information, inventory and recycling rates, goal attainment reports, cyber-security incidents, and incident management events. Management presents key corporate and department goals, summarized financial results, and critical operational performance to Rackspace employees during quarterly, Company-wide Open Book meetings.

Rackspace provides ongoing security awareness guidance and information on securing data, assets, and other sensitive information to Rackspace personnel via security awareness e-mails sent throughout the year. Changes and updates to the security policy are communicated to employees through Company-wide e-mail and through the Global Enterprise Security department. Furthermore, Rackspace employees are trained on the Code of Business Conduct and Ethics annually.

New employees are briefed on the Rackspace security policy during the employee new hire process and each employee signs a security acknowledgement form and confidentiality agreement.

## Description of Information Systems

The embedded parenthetical references are representative of the mapping between the Service Organization Controls and the AICPA Trust Services Principles and Criteria as referenced in Section IV.

## Organization and Management

In order to meet its commitments and requirements as they relate to security and availability, Rackspace has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system. To that end, Rackspace maintains an organizational structure to properly note lines of reporting within each department and job responsibility (**SOC ELC3**).

The Rackspace Leadership Team actively supports information security within Rackspace through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security responsibilities. Security roles and responsibilities of employees, contractors and third party users are defined and documented in the Information Security Policy, ISMS Job Descriptions Policy, and the Compliance Management System manual (**GRP1**) to permit the proper oversight and management of Rackspace's commitment to security and availability to our customers.

Rackspace has assigned and delegated proper responsibilities and authority to members of the Company. Responsibility and accountability for the design, development, implementation, communication and maintenance of Rackspace security and availability policies are assigned to and shared amongst different parts of the organization (ISOC, NET SEC, Compliance, Corporate Security teams) as documented in the Effective Operation of the ISMS & Documentation Policy and Improve Effectiveness of ISMS Procedure and the Compliance Management System Manual **(GRP2)**.

Rackspace has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and requirements as they relate to security and availability. Management requires employees to be subjected to a background check during the hiring process. In the U.S. this includes verifying a social security number, employment verification, a criminal background check, and educational background verification. In the United Kingdom, this includes verifying the legal right to live and work in the UK, employment verification, educational background verification (where applicable), and depending on the position, trade, criminal and/or credit verification. In Hong Kong (HK), this includes verifying an identity card and CV Check. In Australia, this includes verifying employment history, conducting an ID document check and address verification; and, depending on the position, conducting trade, criminal and/or credit verification **(SOC ELC4)**.

Employee competence is a key element of the control environment. Rackspace is committed to training and developing its employees. This commitment to competence is expressed in the Company's personnel policies and related human resource programs. At least annually, the Human Resources Team/Management performs a review of key talent by individual and role to ensure that critical talent is retained and to ensure that the organizational structure is aligned in a way that will support achievement of the Company's objectives and strategies **(SOX ELC1)**. Rackspace ensures that personnel have the knowledge and training needed to perform their duties. New employees go through initial Security training during the New Hire Process **(SOC ELC5)**. In addition, for network security roles, employees need to pass an internal test and industry standard certifications, and new TACACS+ administrator access is provisioned only upon the achievement of a satisfactory score on the TACACS+ Administrator Examination **(GRP3)**.

Personnel responsible for designing, developing, implementing, operating, maintaining and monitoring the system affecting security and availability have the qualifications and resources to fulfill their responsibilities. Before hiring personnel, Rackspace takes actions to address risks to the achievement of objectives by making available the organizational values and behavioral standards in the Rackspace employee handbook. The employee handbook addresses the following topics: Personal Use of Rackspace or Customer Supplies and Equipment, Code of Business Conduct and Ethics, Internet Access guidelines, and Employment practices. The employee handbook is acknowledged by new hires **(SOC ELC1)**. In addition, Rackspace employees are trained on the Code of Business Conduct and Ethics annually **(SOC ELC2)**.

## Communication

Rackspace communicates its security and availability commitments to customers as appropriate. It also communicates those commitments and associated system requirements to internal employees to enable them to carry out their responsibilities. Rackspace communicates to internal and external parties the scope of systems through numerous Compliance documents: SOC reports, Payment Card Industry (PCI) AOC, PCI Executive Summary, ISO 27001 Statement of Applicability, Rackspace Description of Controls, Rackspace Dedicated Frequently Asked Questions (FAQs), and Rackspace Cloud Security FAQ (GRP4).

So that users understand their role in the system and the results of system operation, information regarding system design and operation and boundaries has been prepared and communicated. Rackspace documents the Data center(s) scope and boundaries through its Data Center wiki. The DC wiki is available to Rackspace employees through the Company's intranet.

Data Center policies, procedures, contact personnel, and organization structure by region are also included (GRP5). To ensure that employees understand the Rackspace commitment to security and their responsibilities to uphold that commitment, ongoing training is provided at least annually. Rackspace has instituted a Security Awareness Policy, and the workforce is periodically trained on security expectations (SOC 1.02).

Further support is provided when the Corporate Security team releases periodic communications focusing on immediate security and availability issues and enhancements in security and availability products (GRP6). The Company's commitments and its Information Security Policy are available for review by its employees on the Company intranet.. Reviews are conducted at least annually and updates are performed as needed. At a minimum, the Information Security Policy covers the following topics:

- Risk Management
- Human Resources Security
- Asset Management
- Access Control
- Physical and Environmental Security
- Operations Management
- Information Security Incident Management
- Supplier Relationships
- Compliance
- Enforcement (SOC 1.01)

Moreover, the Chief Information Security Officer holds a "Town Hall" meeting at least quarterly with the Global Enterprise Security teams to discuss and communicate the department's goals and expectations (GRP11). The intent is to ensure alignment, understanding, and communication on the Company's objectives globally. The meeting also serves as an opportunity for employees to express concerns and suggestions, or to ask questions relevant to the Company's objectives.

Weekly, the Foundation Services department communicates to its members a weekly update and status reports on the projects and challenges the division is currently facing. The "weekly buzz" report (**GRP12**) is provided via e-mail. Also, the Rackspace ESWG (Enterprise Security Working Group) meets on a monthly basis to discuss and act on enterprise security concerns. The ESWG group is composed of leaders and representatives from key departments across the Company (**GRP13**).

Communication between Rackspace and external customers is essential to the delivery of Rackspace services, thus the Company's website hosts information pertaining to these services. The Rackspace Service Level Agreement (SLA) is communicated via the Company website and includes provisions for network, hardware, and infrastructure downtime (**GRP7**), while the Rackspace Acceptable Use Policy (AUP) lists activities not allowed by customers who are within the Rackspace network (**GRP10**). Also, Rackspace's commitment regarding the system's security and availability is included in the Rackspace General Terms and Conditions, which is available on the Company website (**GRP8**).

Security commitment and system operation responsibilities are communicated to third parties through the Master Services Agreement and the Hosted Information Addendum (**GRP70**). Monitoring of compliance with commitments and regulatory requirements is conducted via numerous compliance reports (SOC reports, PCI AOC, ISO 27001 certification) that are made available to customers via the MyRackspace™ portal (**GRP9**).

Internal and external system users have been provided with information on how to report security and availability failures, incidents, concerns, and other complaints to appropriate personnel. Escalation procedures are in place and communicated through the customer portal so the customer can get answers to questions and have increasing levels of authority to which to appeal (**GRP14**). In addition, customer support is available 24x7x52 to respond to service requests, questions, monitoring alerts, or service disruptions (**GRP15**).

Internally, an Incident Response process exists to respond to and document physical and cyber security incidents (**SOC 4.01**). The Incident Management team provides documented procedures in the IM intranet website, which establishes point of contact(s) and threshold of incident levels (**SOC 4.04**). Incident events are documented in a database that serves as a central repository; events details at a minimum include the impacted system, incident origin, incident start date and time, impact type, and incident level (**GRP16**).

System changes that affect internal and external system user responsibilities or the entity's commitments and requirements relevant to security and availability are communicated to those users in a timely manner.

Rackspace utilizes a Technical Change Management Process (TCM), which includes participation from individuals representing the various segments of the organization. These individuals are chosen based on performance, knowledge and trustworthiness to make proper decisions and follow the Change Management program effectively. The role of these individuals (called Change Sponsors) is to sponsor potential changes to Rackspace infrastructure that can affect security or availability of services. In addition, the Change Sponsor approves changes directly if the risk score is low or medium, and high-risk changes are approved by the TCM board.



Changes with a medium risk rank are escalated to the Change Sponsor for implementation approval (**SOC 3.03**), and high-risk rank changes are escalated to the Change Sponsor and to the Change Management Board for implementation approval (**SOC 3.04**). Board approval of changes is stored in meeting minutes and the Technical Change Management ticketing system for future review, if necessary.

Communication of infrastructure changes to external customers is provided with at least a 72-hour notice for scheduled non-emergency and non-service disruptive changes (**SOC 3.05**), and with a ten-day notice for non-emergency scheduled changes that could be disruptive to service (**SOC 3.06**). In addition, customer communication is performed for scheduled downtime emergency changes and scheduled upgrades to application components (patches, service packs, utility software, etc.) (**SOC 3.07**).

Internally, infrastructure maintenance changes are scheduled in the calendar tool, which is visible to Rackspace employees (**GRP17**). Hardware-specific maintenance is scheduled in the maintenance calendar tool, where no time periods can be over-booked, and resources are limited for a given time frame (**GRP18**).

After the Change Board has reviewed changes and approved where necessary, the change is migrated into the production environment. Once maintenance has been completed, unexpected issues or failures arising during the implementation process are analyzed and reported to the Change Board.

## **Risk Management and Design and Implementation of Controls**

Rackspace considers the availability of the customer solution from the perspective of network and hardware uptime and the availability of our support services to be of the highest importance. Because of this focus, it regularly reviews controls, processes, and architecture to help facilitate the best available uptime. Rackspace assesses the impact of lost confidentiality, integrity, and asset availability and puts in place and monitors appropriate controls for conformance and effectiveness. Rackspace identifies potential threats that would impair system security and availability commitments and requirements, analyzes the significance of risks associated with the identified threats, and determines mitigation strategies for those risks (including controls and other mitigation strategies).

Rackspace has defined a risk assessment approach. A Security Risk Management Plan provides a methodology that defines Rackspace's risk assessment approach in identifying, analyzing and evaluating risk, and evaluating options for treatment of risks (**GRP19**).

A formal Security risk assessment and management process identifies potential threats to the organization. Management identifies and rates risks (**GRP27**). Identified risks are rated using a risk evaluation process and ratings per the Security Risk Management Plan (**GRP20**). The Risk Management team communicates risk mitigation strategies, including the implementation of new controls, to system owners, and risk recommendation items are followed up to note current state or progress (**GRP25**). Finally, the Risk Management group's recommendations are reviewed and accepted by management (**GRP21**).

In addition, Rackspace identifies and assesses changes (for example, environmental, regulatory, and technological changes) that could significantly affect the system of internal control for security and availability. It reassesses risks and mitigation strategies based on the changes and the suitability of the design and deployment of control activities based on the operation and monitoring of those activities, and updates them as necessary.

A Threat and Vulnerability Analysis team aids in identifying potential concerns that would impair system security (**GRP23**). On an annual basis, Rackspace performs formal risk assessments over its Data Center services systems (**GRP22**). And, at least annually, appropriate levels of management review their internal control frameworks and note any control weaknesses or material changes in controls/environment (**SOX ELC2**). Furthermore, on a periodic basis, the Governance, Risk, and Performance (GRP) team meets with Legal to identify changes that could significantly affect the system of internal control for security and availability.

## Monitoring of Controls

The design and operating effectiveness of controls are periodically evaluated against security and availability commitments and requirements, corrections, and other necessary actions relating to identified deficiencies are taken in a timely manner. Rackspace maintains formal incident response processes concerning both corporate network incidents and incidents affecting customer solutions. Incidents that affect more than one customer or Rackspace operations (Enterprise Impacting) are managed from a centralized tool that provides alerting and escalation paths and procedures, communication procedures and command, control and communication across all Rackspace facilities.

As well, the Company undertakes regular reviews of the effectiveness of the ISMS program, taking into account results of security audits, incidents, and results from effectiveness measurements, and suggestions and feedback from all interested parties. For this purpose Rackspace has established an Information Security Operations Center (ISOC), which is staffed 24x7x52 to identify, monitor, and resolve cyber security incidents. On a periodic basis the ISOC team provides cyber security incident updates to Rackspace leadership (**GRP45**).

## Logical and Physical Access

Rackspace implements various physical security mechanisms to protect its personnel, hardware, network, and data from damage or loss due to unauthorized access. Controlled building access and secure access to specific areas are enforced through the administration of cards and biometric devices.

Access to the data center is restricted through the use of biometric authentication devices (e.g. hand geometry scanner) and key-card/badge devices. Two-factor authentication is used to gain access to the Data Center (**GRP34**), and proximity cards are used at data center facilities to restrict access to only authorized personnel (**SOC 2.01**). Personnel are required to display their identity badges when onsite at Rackspace facilities.

In addition, physical safeguards are in place to restrict access to the server room within the data center **(SOC 2.02)**. Physical access (badge access/biometric access) events are logged and retained for at least 12 months. These logs are available for review in case of an incident or suspicious activity **(GRP36)**. Per the Company's policy, personnel and visitors are required to display their identity badges when onsite at Rackspace Data center facilities. Unescorted visitors are not allowed in sensitive areas **(GRP32)**.

Visitors to Rackspace facilities check in with reception/security before being granted access to Rackspace facilities **(GRP33)**. The visitor log is compiled and retained for 12 months. The visitor logs include the following at minimum: Name, Company, and Date **(SOC 2.03)**.

Customers who are planning to visit a Rackspace data center facility are required to have a valid reason, valid government-issued ID, be approved by an authorized customer contact, and inform the Rackspace management team at least 72 hours prior to the data center visit. Rackspace personnel are on duty at Rackspace data center facilities 24 hours a day, seven days a week.

Appropriateness of physical access to Rackspace data center facilities is reviewed on a periodic basis **(SOC 2.04)**. When physical access is no longer needed due to termination of employment or services, physical access is disabled within the timeframe specified by the Access Termination Standard **(SOC 2.05)**.

Closed circuit video surveillance has been installed at entrance points on the interior and exterior of the buildings housing Data centers and is monitored by authorized Rackspace personnel. The CCTV retention period is at least 90 days **(GRP35)**.

For added security, the Data center facilities are not identifiable from the outside of the building or accessible to unauthorized personnel **(GRP29)**, and security guards are present at the facilities to monitor physical activity and to respond to security incidents **(GRP30)**. In addition, the Data centers have an alarm system at exit and entry points to alert security personnel if a door is forced open or left open **(GRP31)**.

Customers are responsible for implementing physical security controls and environmental controls to protect workstations, servers, and communication hardware which interface with their managed hosting environment at Rackspace and are housed in their facilities or other locations under their control or supervision.

Rackspace policies require users to be specifically authorized to access information and system resources. The Global Enterprise Technology Department (GET) is responsible for security administration functions, including the provisioning and deactivation of employee logical access accounts in internal Rackspace systems.

The Global Data Center Infrastructure (GDCI) team administers the overall access to network infrastructure. Network infrastructure is categorized in two sets, Rackspace's network infrastructure (shared infrastructure) and the customer's network infrastructure. The GDCI team manages Rackspace's network infrastructure, whereas the NetSec team manages the customer's network infrastructure.

The stability of the Rackspace network (shared infrastructure and customer infrastructure) is essential to meeting the Company's delivery of uptime and reliability commitments to our customers. Rackspace takes measures to ensure that all employees with access to the network infrastructure have the appropriate level of knowledge and experience to make configuration changes with minimal security risks and service disruptions to the network itself.

New administrator access to network devices supporting Rackspace infrastructure is granted through the new user creation process. Access is role based and deviations require manager approval (**SOC 6.01**). The GDCI team maintains a series of examinations that are used to test an employee's technical ability and knowledge of the Rackspace network infrastructure for the purpose of determining the level of access the employee will be granted.

Administrator access to networking devices is controlled via the use of an access control system that provides authentication, authorization, and accountability services (TACACS+). Rackspace secures access to core networking infrastructure utilizing inherent access control functionality in TACACS+ software (**SOC 6.02**). User activity is controlled and restricted by defining granular authorization privileges in TACACS+. Employees' authorization privileges are based on the examination results administered by the GDCI team as part of the new user creation process. In addition, TACACS+ access lists are reviewed on a quarterly basis to verify those users on the list still require access to network devices (**SOC 6.03**).

Independent domain controllers are in place for the administration and segregation of the Company's corporate network and customer environments. Access to the Company's network is restricted to authorized personnel only, and authentication mechanisms are in place to enforce such restrictions.

Rackspace's internal tools and equipment logically reside within the corporate network, thus access to these resources is limited to connections originating from within the network. Employees can access internal resources by initiating the connection from Rackspace's offices, data centers, or by remotely connecting into the network. Although remote network access is permitted, two-factor authentication is used to remotely connect to the Rackspace corporate network (**SOC 6.04**).

Employee access to the Rackspace corporate network and to customer environments is administered via the Corporate Active Directory and the Intensive Active Directory, respectively. In both cases, Active Directory maintains appropriate segregation of duties through the use of various delegation boundaries (**SOC 6.05**).

Human Resources is the only division authorized to request corporate network accounts for new employees. A request is initiated by adding a job position within the Global People System (HR database) to reflect the hire of a new employee. Nightly, the Corporate Active Directory syncs with the GPS system to determine newly hired employees in need of a network account, and searches for terminated employees whose access needs to be removed from the network. By following this process, Rackspace ensures that Human Resources is the authoritative source for the proper granting and removal of employees' logical access to corporate resources. In addition, this process ensures that Corporate Active Directory access is disabled in a timely manner (**SOC 6.06**) for employees who are no longer with the Company.

When an employee's job responsibilities change or the employee transfers to a new department, the individual's manager contacts the GET department to modify the transferred employee's access rights to those that are commensurate with the employee's new position and responsibilities.

Employee access to the corporate network is granted and managed by adding the employee's network account into an AD group or several groups. Management has implemented a process to review each of the members of a group by the group owner to ensure access is still appropriate. The Corporate Active Directory user access list is reviewed on an annual basis. Any discrepancies found are corrected in a timely manner **(SOC 6.07)**.

Rackspace has established a minimum password baseline configuration for its Corporate Active Directory, including the following parameters **(SOC 6.08)**:

- Password history (24 previous iterations)
- Maximum age 90 days
- Minimum age one day
- Minimum length seven characters
- Complexity: Upper case, lower case, use of numbers 0-9, use of special characters
- Account lockout duration: 30 minutes
- Account lockout threshold: six attempts
- Account reset: 30 minutes

For the Intensive Active Directory, Rackspace has established a minimum password baseline configuration, including the following parameters **(SOC 7.01)**:

- Password history (six passwords remembered)
- Minimum length seven characters
- Complexity: upper case, lower case, use of numbers 0-9
- Account lockout duration: 30 minutes
- Account lockout threshold: five invalid attempts

Also, Intensive Active Directory passwords used by Rackspace employees are rotated at least every 24 hours **(SOC 7.02)**. After an employee has been granted a corporate network account, then an Intensive Active Directory account can be created. New user accounts within the Intensive Active Directory are created based on a person's job function and/or manager approval **(SOC 7.03)**.

The Intensive Active Directory user access list is reviewed on a quarterly basis. Any discrepancies found are corrected in a timely manner **(SOC 7.04)**. An automated process is in place to review each user's current title and group division to ensure access is still appropriate. For users whose title or division is not within a role that supports customer environments, the user's manager approval is required to maintain access for the next three months.

Employee access to customer environments is restricted through several layers of authentication mechanisms and systems. Rackspace utilizes inherent access control functionality within Intensive Active Directory and CORE to secure access to customer servers **(SOC 7.05)**. Systems restricting access to customer devices operate a role-based access functionality to provide appropriate segregation of duties within the Company's workforce. CORE is the Company's customer service platform, and while most of the Rackspace personnel have access to this system, only appropriate personnel have access to see sensitive information regarding customer devices.

Access to hosting environments is administered by allowing connections from a restricted group of computers only **(SOC 7.06)** Rackspace personnel authenticate to a server farm (bastion servers) prior to authentication and connection to a customer device. A bastion server is a gateway and a layer of security positioned between Rackspace infrastructure and the customer infrastructure; it enables the delivery of Rackspace's Fanatical Support while protecting the customer environment. Each Rackspace data center has its own set of bastion servers and access is restricted to members of a specific access group. Two-factor authentication is used to connect to the bastion servers **(GRP37)**.

Bastions provide security to the customer environment by restricting access, ensuring the Rackspace infrastructure interfacing with the customer environment has the most up to date OS patches and up to date anti-virus engine **(GRP42)**, and selected activity is logged.

Customer environments are isolated from one another via the use of VLAN and separate broadcast domains **(SOC 7.07)**. Virtual networks (VLAN) are used to logically segment customers on the Rackspace network into different broadcast domains so that packets are only switched between ports that are designated on the same VLAN, thus ensuring segmentation of networks amongst Rackspace customers.

Individual Managed Hosting customer configurations utilize dedicated hardware for servers, firewalls, and load-balancers **(SOC 7.08)**. In other words, dedicated managed hosting customers are assigned their own hardware and are given full administrative control to this infrastructure. Customer firewalls delineate the boundary between Rackspace shared infrastructure and the customer environment. Rackspace fully manages the administration of shared infrastructure and Rackspace customers retain full administrative rights and control of their environments. The customer is therefore considered the primary system administrator of their environment. By outsourcing the hosting to Rackspace, the customer has delegated responsibility for managing the infrastructure components of their environment.

Customers have full access to log into their servers remotely using secure shell (SSH) or Windows Remote Desktop, depending on the platform. For customers that selected a firewall, a default Access Control List (ACL) rule set has been created to be deployed in newly configured firewalls. Rackspace communicates the default ACL configuration to the customer via a CORE ticket **(SOC 7.09)**. In addition, Rackspace will communicate the default firewall rule set as part of the customer implementation call agenda and it is available for review by the customer via the customer portal.

A firewall rule set can be modified by employees that have been granted an account within the TACACS software, since TACACS administers the access to Rackspace's networking devices. For customer firewalls, modifications to the rule set are also available via the

customer portal (MyRackspace™ portal). Only authorized employees have the ability to access the customer firewall manager, which is the module that allows such modifications. Changes to a customer firewall via the MyRackspace™ portal are logged and available for review **(SOC 7.10)**; this include changes made by Rackspace employees and changes made by Rackspace customers.

The Rackspace network has several mechanisms and controls in place to safeguard its security and availability. For example, the ISOC team has implemented an intrusion detection system (IDS) to detect and act upon the detection of anomaly network behavior due to unauthorized software or malicious attacks **(GRP41)**. Also, Rackspace utilizes data loss prevention software to scan for sensitive information in outgoing transmissions **(GRP39)** to ensure the confidentiality of this type of data.

To reinforce our objective to secure data, the Company's Security Travel Standard defines mandatory security measures for when full encryption of removable media is required **(GRP40)**. This definition is stipulated and taken into consideration the city or country of destination as well as purpose of the travel, such as the event or conference.

Secure connections to Rackspace ticketing systems and the employee HR system is important in order to maintain the confidentiality of the information housed in this system, therefore the customer service platform and Global People System are encrypted using strong cryptography protocols such as SSN, VPN or SSL/TLS **(GRP24)**.

## **Systems Operations**

Vulnerabilities of system components to security and availability breaches and incidents due to malicious acts, natural disasters, or errors are monitored and evaluated and countermeasures are implemented to compensate for known and new vulnerabilities. Known vulnerabilities are counter measured by making accessible to customers a Windows and Linux server with the most up-to-date patches ready to download and install **(GRP67)**.

In order to trace malicious acts or trace errors in the network, an access control system is used to log administrator activity to network devices. Logged activity includes username, successful/unsuccessful login attempts, and timestamp. These logs are retained for one year, and are available for review in case of an incident or suspicious activity **(GRP43)**. Audit logs recording user activities, exceptions, and information security events are produced and kept for an agreed period to assist in future investigations and access control monitoring. Bastion logs are kept for a 90-day period, and are available for review in case of an incident or suspicious activity. Log information includes: username, timestamp, successful/unsuccessful login attempts **(GRP44)**.

Security and availability incidents, including logical and physical security breaches, failures, concerns, and other complaints, are identified, reported to appropriate personnel, and acted on in accordance with established incident response procedures. Rackspace has an incident management hotline for employees to report applicable incidents **(SOC 4.03)**.

Incident events are documented in a database that serves as a central repository. Once an event is created, it is assigned a unique identifier, and an e-mail is sent to applicable Rackspace personnel for notification and status update(s) **(SOC 4.05)**. When an incident is resolved, the ticket is closed, documenting the time of the resolution **(SOC 4.06)** to note the time it took to contain the incident and resolve the issue.

A summary of physical and cyber security incidents is compiled and distributed to the Global Security team on a weekly basis **(GRP48)** to make leadership and appropriate personnel aware of current security challenges and concerns.

Natural disasters have the potential to disrupt Data centers and systems and data housed within these systems. A data backup process is in place for customers who have subscribed to the managed backup service. The backup schedule is based on the backup frequency configured in the backup utility software **(SOC 8.01)**.

To ensure that backups are being performed and not skipped due to bad media or equipment, Rackspace has implemented an automated failure resolution process in order to mitigate the risk of faulty media **(GRP47)**. The backup utility software is configured to replace media after a set number of failed attempts to write to media.

Monitoring and information on the status of backups can be performed via the MyRackspace™ portal. Customers are encouraged to log into the customer portal to review their most recent backup status (success or failure) status and their current size or volume of backed up information **(GRP46)**.

## **Change Management**

Rackspace technical infrastructure is continuously evolving to deliver a reliable and world-class global infrastructure to its customers. A structured change management process is documented within the Rackspace Technical Change Management Policy to prevent and reduce service disruptions of Rackspace's shared infrastructure. Service disruptions may occur due to changes such as upgrades, maintenance, and fine-tuning.

Rackspace shared infrastructure represents any component of the communications network or physical environment that is not customer specific. Customer-specific communications equipment represents the demarcation of shared infrastructure. Rackspace customers use this shared infrastructure to gain the economies of scale cost advantage benefits that shared infrastructure offers for applicable types of equipment. Examples include core routers, switches, SAN fabric, backup infrastructure, and Internet backbone connections.

Rackspace has instituted a Technical Change Management Policy, which proposed changes to the infrastructure must adhere to. The policy is reviewed on an annual basis **(SOC 3.01)**. Prior to implementation of changes to the production environment, infrastructure changes undergo testing when feasible **(SOC 3.02)**. For this purpose, Rackspace has implemented separate test and production environments for its bastion servers and GDCI networking infrastructure **(GRP51)**.



Testing is performed once the Change Sponsor has developed a test plan, relevant technical personnel have vetted this plan, and all necessary equipment is obtained. Typically, testing is performed in a segregated test lab on the Rackspace campus. The level of testing performed is dependent on the nature of the project being implemented and follows the vendor's recommended test strategy, when applicable.

Proposed changes to technical infrastructure are assessed to determine the level of approval and communication required before implementation. Assessment rating consists of the review of the change across three dimensions: impact, likelihood, and redundancy. A Risk rating assessment will place a change between a tier 1, tier 2, tier 3, or tier 4 groups.

Low risk changes fall within the tier 4 group, medium risk changes fall within the tier 3 group, and high risk changes fall within the tier 2 and tier 1 groups. Technical infrastructure changes with a medium risk rank are escalated to the Change Sponsor for implementation approval (**SOC 3.03**), and technical infrastructure changes with a high-risk rank are escalated to the Change Sponsor and to the Change Management Board for implementation approval (**SOC 3.04**).

Proposed non-emergency changes that are scored as high priority are presented and reviewed at the monthly Change Board Meeting. The Change Board approves high impact changes and those medium or low impact changes that have been escalated by a Change Sponsor prior to the scheduled maintenance. From change inception to finalization, the Change Board works with relevant stakeholders to validate potential interdependencies have been considered and appropriately addressed.

After the Change Board has reviewed changes and approved where necessary, the change is migrated into the production environment. Once maintenance has been completed, unexpected issues or failures arising during the implementation process are analyzed and reported to the Change Board.

The Risk Management team evaluates the need for changes on a constant basis. This continuous evaluation serves to ensure Rackspace's commitment to security and availability of our products and services. For critical or high severity findings resulting from risk assessments, a change request is created based on the identified need (**GRP50**), and the top five risks resulting from risk assessments are communicated to our Security Leadership (**GRP49**).

Risk assessments are stored in a centralized database system to preserve the information's confidentiality, integrity and availability. In addition, Rackspace utilizes a centralized ticketing system that incorporates problem management, incident management, and change management (**GRP68**) for easy correlation and forecast problem to prevent its occurrence.

## **Availability**

Current processing capacity and usage are maintained, monitored and evaluated to manage capacity demand, and to enable the implementation of additional capacity to help meet availability commitments and requirements. Redundant lines of communication exist to telecommunication providers (**GRP53**) to protect against availability issues. In addition, fully

redundant routing and switching equipment is utilized for Rackspace's core network infrastructure **(GRP56)**. Rackspace internal policies and processes mandate that the use of resources shall be monitored and tuned, and projections made of future capacity requirements to ensure the required system performance.

Environmental protections, software and recovery infrastructure are designed, developed, implemented, operated, maintained and monitored to meet availability commitments and requirements. The Data Center facilities are equipped with redundant HVAC units to maintain consistent temperature and humidity levels **(GRP52)** and to protect against environmental risks. Data centers are equipped with sensors to detect environmental hazards, including smoke detectors and floor water detectors, where chilled water systems are used as coolant **(GRP59)**. In addition, Data center facilities are equipped with raised flooring (DFW1, DFW2, DFW3, IAD2, IAD3, ORD1, LON1, LON3, LON3DH4, HKG1, SYD2, SYD4) or an indirect air cooling system (LON5) **(GRP60)**.

To prevent and mitigate the risk of loss of data and equipment due to a fire, Data Center facilities are equipped with fire detection and suppression systems **(GRP61)**, and fire detection systems, sprinkler systems, and chemical fire extinguishers are inspected at least annually **(GRP62)**. To mitigate data loss due to power failures and/or fluctuations, Data Centers are equipped with uninterruptible power supplies (UPS) systems and diesel generators **(GRP55)**. The UPS systems are inspected and/or serviced at least annually **(GRP63)**, and generators are tested at least every 120 days and serviced at least annually **(GRP64)**.

Rackspace has developed and maintains a process to address its business continuity plan throughout the organization. This plan addresses the information security requirements needed for the Company's continuity in a disaster scenario. It plans for the maintenance and/or restoration of operations to ensure availability of information and continuity of critical business processes. More specifically, a Data Center Business Continuity plan exists, and provides the global business continuity plan for Rackspace data centers to manage significant disruptions to its operations and infrastructure **(GRP65)**.

Procedures supporting system recovery in accordance with recovery plans are periodically tested to help meet availability commitments and requirements. Rackspace tests and updates its business continuity plans regularly to confirm that they are up to date and effective **(GRP66)**. Tests include full walkthroughs of plans onsite to train staff on emergency events and to ensure plans are thorough enough in the case of an emergency. Tests are recorded, saved and used as learning exercises for future tests or emergencies.

## **Trust Services Criteria and Related Controls**

Although the trust services criteria, related controls and management responses to deviations, if any, are presented in Section IV, "Trust Services Security and Availability Principles, Criteria, Related Controls, and Tests of Controls," they are an integral part of Rackspace's system description.

**Section IV – Trust Services Security and Availability**  
**Principles, Criteria, Related Controls, and Tests of Controls**

## **Section IV – Trust Services Security and Availability Principles, Criteria, Related Controls, and Tests of Controls**

### **Testing Performed and Results of Tests of Entity-level Controls**

In planning the nature, timing and extent of our testing of the controls specified by Rackspace, we considered the aspects of Rackspace's control environment, risk assessment processes, information and communication and management monitoring procedures and performed such procedures as we considered necessary in the circumstances.

### **Description of Information Systems**

On the pages that follow, the description of the applicable Trust Services Criteria and the controls to meet the criteria have been specified by, and are the responsibility of Rackspace. The testing performed by EY and the results of tests are the responsibility of the service auditor.

## Attachment E

Answer to question C-SLC-001, C-SLC-003, C-ICD-008 and C-ICD-009.

### **Pricing & Methodology**

Fischer International Identity has provided a detailed price quote representing the Virginia Commonwealth University's investment for either an On Premise or Cloud Hosted Identity Management Solution for the reported FTE's/users. Pricing is determined based on the User Type and Deployment model chosen by the organization.

### **1. License and Deployment Model**

Student FTE pricing was designed with the assistance of colleges and universities to create a clear, predictable, and easy-to-administer license model that is based solely on the institution's Student FTE enrollment. It provides the benefits of an "**enterprise license**" but at significantly-reduced cost.

- License fees are based only on the FTE Student enrollment; there are no license fees for Authorized Non-FTEs users (e.g., faculty, staff, alumni, applicants, guests, parents, etc.).
- The Authorized Non-FTEs User population is set at 10-times the Student FTE count.
- Inactive users do not consume licenses (e.g., users that are stored in the Fischer system for archival purposes)
- There are no license or maintenance fees for connectors (excluding connectors for custom or non-commercially viable systems).
- Fischer does not require True-up until actual Student FTE exceeds licensed FTE by 5%.

Headcount pricing is based on the actual number of Authorized Users to be managed and their types; fees are deeply discounted for users who are not students, faculty, or staff. An "Authorized User" means person whose Personal Information, identity data and/or access privileges are managed by the Fischer solution pursuant to a master license agreement. The three types of Authorized Users are below:

- "Internal Authorized User" includes any Authorized Users who are Licensee's employees, consultants, contractors, outsourcers, or exclusive agents and any other Covered Persons not meeting the definition of an External Authorized User or Community Authorized User; for Education, Internal Authorized Users also include students, faculty and staff.
- "External Authorized User" includes any Authorized Users who are third-party providers, suppliers, customers, vendors or independent agents.
- "Community Authorized User"(available only to educational institutions) includes alumni, applicants, guests, parents, corporate partners, researchers at external institutions, and other types of users not defined above.

The headcount model has the following terms:

- License Fees: User licenses are "per named user." License fees vary based on the User Type per Section 2 below. Connectivity license fees are \$10,000.00 USD per connector and are waived for all Fischer connectors that ship with the product.

- User Types: User License Fees are based on the type of Authorized User: Internal, External, Community. This tiered license model reduces the cost to support populations that do not use the solution frequently and significantly increase product utilization at minimal cost.
- Inactive or archived identities that are stored but not being actively managed in any way by the Fischer product or service are neither counted as users nor carry a headcount fee.
- Annual Maintenance Fees: The Annual Software Maintenance fee is based on the total Software License Fee and connectivity-related maintenance fees. While connectivity license fees may be waived, a 22% annual maintenance fee is charged based on the value of each unique connector.
- Connector Development: If Fischer does not have an existing connector for a needed system, connector development fees will be waived for up to three (3) commercially-viable systems. Fischer reserves the right to charge development fees for additional commercially-viable connectors. License fees and development charges apply to all other connectors (e.g., custom connectors, non-commercially viable connectors).
- Note: Commercially-viable" is defined as a COTS system that, in Fischer's sole determination, will be needed by a reasonable number of other potential Fischer customers. The decision to waive development fees is based substantially on the projected or reported application market share and application version (e.g., application age, EOL, etc.).
- License Administration / True-up: The total number of active Authorized Users being managed by the Fischer product or service may vary up to ten percent (10%) before additional licenses must be purchased

### Deployment Models

Fischer offers its IdM capabilities in either an on-campus deployment or using Fischer's Identity as a Service® Cloud, a software-as-a-service (SaaS) model.

- On-campus deployments are ideal for institutions that prefer self-administration and management and desire to extend the solution without vendor professional services. On-campus deployments are generally sold with a perpetual software license for a specified number of users, and this model has a base annual maintenance fee of 22%.
- Hosted/Managed deployment in Fischer's Identity as a Service® Cloud enables institutions to outsource their IAM infrastructure and administration activities. For an annual subscription fee, Fischer performs all daily activities and provides a given number of hours of monthly services for performing routine tasks. The IaaS® option provides a term license for five (5) years for a specified number of users; a shorter term may be requested but may affect the price.

## **2. Total Implementation Costs**

Based on the preliminary technical data provided by the institution, and additional population data retrieved from IPEDS and SCHEV, the following estimated implementation costs are provided:

On Premise Deployment: \$112,000.00  
Identity as a Service Deployment: \$110,775.00

### **3. Total Annual Costs**

#### **IdM Modules Require:**

- Password Reset and Synchronization
- Auto Role and Account Management
- Self Service Portal
- Mobile IAM
- Compliance and Audit Reporting
- Privileged Account Access

Based on the user population data provided by the institution, the following estimated annual costs are provided:

#### FTE MODEL (28,456 FTEs – Reported by SCHEV)

On Premise Deployment (One Time Charge) Year 1: \$620,340.80

On Premise Deployment Annual Maintenance: \$136,474.98

- Average Annual Per Internal User \$21.80

Identity as a Service Deployment Annual Subscription: \$385,578.80

- Average Annual Per Internal User \$13.55

#### HEADCOUNT (32,000 Students/8,264 FT Faculty & Staff/6,515 PT Staff/174,573 Alumni)

On Premise Deployment (One Time Charge) Year 1: \$605,135.49

On Premise Deployment Annual Maintenance: \$139,729.81

- Average Annual Per Internal User \$12.11

Identity as a Service Deployment Annual Subscription: \$312,908.29

- Average Annual Per Internal User \$9.30

### **4. Annual Maintenance and Support Costs**

Annual software maintenance includes bug-fixes, minor releases and major releases for licensed software and technical support. If the client selects the Identity as a Service deployment model, there are no additional annual charges for maintenance or support. If the client selects the On Premise Deployment Model, the Annual Maintenance fee is 22% of the license charge.

On Premise Deployment Annual Maintenance:

FTE MODEL: \$136,474.98

HEADCOUNT: \$139,729.81

### **5. Training Costs**

Basic and advanced administrator training is included in the implementation service costs provided above. Additional training can be added as needed at the standard professional services rate.

### **6. Hardware Costs**

There are no additional hardware costs associated with the standard Identity as a Service Deployment Model.

Fischer does not provide hardware for the On Premise Deployment Model.

### **7. Other Costs**

T&E are not included in the estimated costs provided.

Cost for additional users based on deployment and pricing model selected.





**VIRGINIA COMMONWEALTH UNIVERSITY**  
**Identity Management Project**  
**Full Time-Equivalent Student Pricing Model**  
**Pricing Valid through 3/1/17**

**Pricing Model:** FTE

**IdM Modules Required:**

- o Password Reset & Synchronization
- o Auto Role & Account Management
- o Self Service Portal
- o Mobile IAM
- o Compliance & Audit Reporting
- o Privileged Account Management

<b>On-Premise Deployment Model (One-time License Charge)</b>				
<b>Software License Costs<sup>1,2</sup></b>	<b>Count</b>	<b>List</b>	<b>Discount</b>	<b>Net</b>
Student FTEs (Reported to Educause)	28,456	\$1,240,681.60	50%	<b>\$620,340.80</b>
Annual Maintenance (22%)		\$272,949.95	50%	<b>\$136,474.98</b>
<b>Year 1 Software &amp; Maintenance Costs</b>		<b>\$1,513,631.55</b>		<b>\$756,815.78</b>
<b>Estimated Implementation Costs<sup>3</sup></b>	<b>Hours</b>	<b>List</b>	<b>Discount</b>	<b>Net</b>
Implementation Services	640	\$160,000.00	30%	\$112,000.00
<b>Total Year 1 Cost</b>				<b>\$868,815.78</b>

<b>Identity as a Service® Model (SaaS Subscription)</b>				
<i>(Based on above information. Initial Term: 5 Years)</i>				
<b>Annual Subscription Fee<sup>1,2</sup></b>	<b>Count</b>	<b>List</b>	<b>Discount</b>	<b>Net</b>
Student FTEs (Reported to Educause)	28,456	\$771,157.60	50%	<b>\$385,578.80</b>
<b>Total Annual Fees</b>		<b>\$771,157.60</b>		<b>\$385,578.80</b>
<b>Estimated Implementation Costs<sup>3</sup></b>	<b>Hours</b>	<b>List</b>	<b>Discount</b>	<b>Net</b>
Implementation Services	633	\$158,250.00	30%	\$110,775.00
<b>Total Year 1 Cost</b>				<b>\$496,353.80</b>

**Cost for Additional FTEs\***

- One-time License: \$21.80 (Per-FTE Cost)
- Annual IaaS® Subscription: \$13.55 (Per-FTE Cost)

\* New license prices are valid for three (3) years from the effective date of Agreement. Maintenance not included.



**VIRGINIA COMMONWEALTH UNIVERSITY**  
**Identity Management Project**  
**Full Time-Equivalent Student Pricing Model**  
**Pricing Valid through 3/1/17**

**<sup>1</sup>FTE Pricing Notes:**

*Note: Users are calculated based on Student Full-time Equivalent (FTEs) numbers and not headcount for individual user types (e.g., student, faculty, staff, alumni, etc.)*

<b>Criteria</b>	<b>Description</b>
User License Fees	Student FTE only. Other Authorized user populations (students, faculty, staff, alumni, guests, etc.) are included without fee up to 10-times licensed Student FTE count.
Connectivity License and Development Fees	No per-system connectivity or maintenance fees. New connectors developed without charge for up to 5 commercially-viable systems.
License Count Variance	5%: Student FTE count may exceed license count up to 5%.
Cost Increase "Resilience"	Excellent: No additional license/maint. fees related to growth in: <ul style="list-style-type: none"> <li>• non-FTE user populations</li> <li>• systems (with existing Fischer connectors)</li> </ul>
License Administration	Simple: <ul style="list-style-type: none"> <li>• Only FTEs need be tracked.</li> <li>• Unlimited growth for non-Student FTE populations (e.g., alumni)</li> </ul>

**<sup>2</sup>Connected Systems**

The implementation costs quoted herein assume that the systems below leverage existing Fischer connectivity or are commercially-viable and covered under the "Connected Systems" Terms below.  
AD,Banner,Oracle E-Directory,Google Apps,Blackboard,C-CURE,CBORD

Fischer's FTE Pricing Model includes connectivity and associated maintenance for systems within Fischer's connectivity library. If Fischer does not already have a connector for a commercially-viable system that is required by the institution, Fischer will develop it without charge for up to three (3) commercially viable systems (see definition below). Fischer reserves the right to charge for connectivity development and associated maintenance fees for connectors for any additional connectors. Connector fees for systems that are not commercially-viable for Fischer will be quoted separately. Software maintenance fees apply to all UNIQUE connectors in use and are valued at \$10,000.00 USD per unique connector.

NOTE: The development and maintenance fees for connectors is based on UNIQUE system (version/release), not per instance or connection point. For example, the cost basis for connecting to six (6) Oracle 11g Release 2: 11.2.0.1 databases is one (1) and not six (6).

NOTE: "Commercially-viable" is defined as a COTS system that a reasonable number of other potential Fischer customers will need supported. The decision to waive development costs is made on a case-by-case basis and is based in part on projected or reported application market share and application version (e.g., application age, EOL, etc.).

**<sup>3</sup>Implementation Services Estimate & Assumptions**

Implementation services prices are for estimation purposes only and are not guaranteed. A formal quote for implementation services will be provided following a discovery workshop that commences upon contract execution. T&E are not included in estimate.



**VIRGINIA COMMONWEALTH UNIVERSITY**  
**Identity Management Project**  
**Full Time-Equivalent Student Pricing Model**  
**Pricing Valid through 3/1/17**

<b>Solution Requirements</b>	<b>On-Premise (QTY)</b>	<b>IaaS® (QTY)</b>
<b>Environment Specifics</b>		
Number of Environments	2	0
Additional HA Servers	2	0
Number of Global Identity Gateways	0	3
Number of MS Password Filters	0	0
<b>Modules</b>		
Password Management	Yes	Yes
Provisioning	Yes	Yes
HPAM	No	No
Federation	No	No
<b>Workshop Options</b>		
Password Management Workshop	Yes	Yes
Provisioning Workshop	Yes	Yes
HPAM Workshop	No	No
Federation Workshop	No	No
<b>Solution Specifics</b>		
Number of Initiation Points (Source of Authority)	1	1
Number of Password Management Targets	3	3
Number of Administrative Provisioning Targets	0	0
Number of Administrative Provisioning Workflows per target	0	0
Number of Automated Provisioning Target	6	6
Number of Automated Provisioning Workflows per target	4	4
Number of HPAM Account Types	0	0
Total Number of Unique Connected System Definitions	7	7
Number of Approval Configurations	3	3
Number of Selectable Resources	6	6
Number of Resource Group Configurations	2	2
Number of Policies	50	50
Number of Organizations	1	1
Is IdP on Premise or IaaS	None	None
Number of IdPs	0	0
Number of Shibboleth SPs to Shibboleth Applications	0	0
Number of Discovery Services for Shibboleth SPs	0	0
Number of SAML enabled Federation Targets (SPs)	0	0
Number of verified SFL enabled Federation Targets (SPs)	0	0
Number of non-verified SFL enabled Federation Targets (SPs)	0	0
Number of Attribute Management Processes	0	0
Number of On-Going Attribute Management Processes	0	0
Include Post Implementation Services	Yes	Yes
User Account Load	Custom	Custom
<b>Training</b>		
Basic Training	No	No
Advanced Training	No	No
Kiosk UI Training (Train the Trainer)	Yes	Yes
Pin Reset UI Training (Train the Trainer)	Yes	Yes
Help Desk UI Training (Train the Trainer)	Yes	Yes
Self Service Access Management UI Training (Train the Trainer)	Yes	Yes
HPAM UI Training (Train the Trainer)	No	No
Federation Configuration Training	No	No



**VIRGINIA COMMONWEALTH UNIVERSITY**  
**Identity Management Project**  
**Headcount Pricing Model**  
**Pricing Valid Through 3/1/2017**

**Pricing Model: HEADCOUNT**

**IdM Modules Required:**

- o Password Reset and Synchronization
- o Auto Role & Account Management
- o Self Service Portal
- o Mobile IAM
- o Compliance & Audit Reporting
- o Privileged Account Management

**On-Premise Deployment Model (One-time License Charge)**

<b>Software License Costs</b>	<b>Count</b>	<b>List</b>	<b>Discount</b>	<b>Total</b>
Internal Users: Students	32,000	\$775,040.00	50%	\$387,520.00
Internal Users: Faculty/Staff/Contract.	8,264	\$200,154.08	50%	\$100,077.04
External Users	6,515	\$23,669.00	50%	\$11,834.50
Applicants	0	\$0.00	50%	\$0.00
Guests/Other	174,573	\$211,407.90	50%	\$105,703.95
Connectors <sup>2</sup> : (See Page 2)	6	\$60,000	100%	\$0.00
<b>Sub Total Software</b>		<b>\$1,270,270.98</b>		<b>\$605,135.49</b>
<b>Annual Maintenance</b>		<b>\$279,459.62</b>	<b>50%</b>	<b>\$139,729.81</b>
<b>Year 1 Software &amp; Maintenance Costs</b>		<b>\$1,549,730.59</b>		<b>\$744,865.30</b>
<b>Estimated Implementation Costs<sup>3</sup></b>	<b>Hours</b>	<b>List</b>	<b>Discount</b>	<b>Net</b>
Implementation Services	640	\$160,000.00	30%	\$112,000.00
<b>Total Year 1 Cost</b>				<b>\$856,865.30</b>

**Identity as a Service® Model (SaaS Subscription)**

*(Based on above information. Initial Term: 5 Years)*

<b>Subscription Fees</b>	<b>List</b>	<b>Discount</b>	<b>Total</b>
Annual Subscription Fee (5 Year Contract)	\$625,816.57	50%	<b>\$312,908.29</b>
<b>Total Annual Fees</b>	<b>\$625,816.57</b>		<b>\$312,908.29</b>
<b>Estimated Implementation Costs<sup>3</sup></b>	<b>Hours</b>	<b>List</b>	<b>Discount</b>
Implementation Services	633	\$158,250.00	30%
<b>Total Year 1 Cost</b>			<b>\$423,683.29</b>

**Pricing for Additional Users:**

New licenses may be added per the pricing below. New license prices are valid for three (3) years from the effective date of the license agreement. Maintenance (22%) not included.

	<b>One-time License</b>	<b>Annual SaaS Subscription</b>
	<b>(Per-User Cos (Per-User Cost))</b>	
Students	\$12.11	\$9.30
Faculty/Stf.	\$12.11	\$9.30
External	\$1.82	\$1.40
Applicant	\$0.61	\$0.47
Guests/Other	\$0.61	\$0.47



**VIRGINIA COMMONWEALTH UNIVERSITY**  
**Identity Management Project**  
**Headcount Pricing Model**  
**Pricing Valid Through 3/1/2017**

**User License Definitions (headcount pricing model):**

Internal user: For Education, a student, faculty, or staff member, regardless of their location or whether the student matriculated through another school.

External User: For Education, any user who does not meet the criteria of an Internal User, Bridge User, Recruiting User, or Inactive user. For example, alumni, external contractors, external researchers, commercial partners, etc., are External Users.

Community User: Community Users includes alumni, applicants, guests, parents, corporate partners, researchers at external institutions, and community outreach users.

**<sup>2</sup>Connected Systems**

The implementation costs quoted herein assume that the systems below leverage existing Fischer connectivity or are commercially-viable and covered under the "Connected Systems" Terms below.

*AD, Banner, Oracle E-Directory, Google Apps, Blackboard, C-CURE, CBORD*

Fischer's Headcount Model waives connectivity license fees for connectors that ship with the product's connectivity library. If Fischer does not already have a connector for a commercially-viable system that is required by the institution, Fischer will develop it without charge for up to three (3) commercially viable systems (see definition below). Fischer reserves the right to charge connectivity development fees for additional commercially-viable connectors that do not yet ship with the Fischer product. Connector fees for systems that are not commercially-viable for Fischer will be quoted separately. Software maintenance fees apply to all UNIQUE connectors in use and are valued at \$10,000.00 USD per unique connector.

NOTE: The development and maintenance fees for connectors is based on UNIQUE system (version/release), not per instance or connection point. For example, the cost basis for connecting to six (6) Oracle 11g Release 2: 11.2.0.1 databases is one (1) and not six (6).

NOTE: "Commercially-viable" is defined as a COTS system that a reasonable number of other potential Fischer customers will need supported. The decision to waive development costs is made on a case-by-case basis and is based in part on projected or reported application market share and application version (e.g., application age, EOL, etc.).

**<sup>3</sup>Implementation Services Estimate & Assumptions**

Implementation services prices are for estimation purposes only and are not guaranteed. A formal quote for implementation services will be provided following a discovery workshop that commences upon contract execution. T&E are not included in estimate.

The implementation services in this quote are based on the information on the following page:



**VIRGINIA COMMONWEALTH UNIVERSITY**  
**Identity Management Project**  
**Headcount Pricing Model**  
**Pricing Valid Through 3/1/2017**

<b>Solution Requirements</b>	<b>OnPrem (QTY)</b>	<b>IaaS® (QTY)</b>
<b>Environment Specifics</b>		
Number of Environments	2	0
Additional HA Servers	2	0
Number of Global Identity Gateways	0	3
Number of MS Password Filters	0	0
<b>Modules</b>		
Password Management	Yes	Yes
Provisioning	Yes	Yes
HPAM	No	No
Federation	No	No
<b>Workshop Options</b>		
Password Management Workshop	Yes	Yes
Provisioning Workshop	Yes	Yes
HPAM Workshop	No	No
Federation Workshop	No	No
<b>Solution Specifics</b>		
Number of Initiation Points (Source of Authority)	1	1
Number of Password Management Targets	3	3
Number of Administrative Provisioning Targets	0	0
Number of Administrative Provisioning Workflows per target	0	0
Number of Automated Provisioning Target	6	6
Number of Automated Provisioning Workflows per target	4	4
Number of HPAM Account Types	0	0
Total Number of Unique Connected System Definitions	7	7
Number of Approval Configurations	3	3
Number of Selectable Resources	6	6
Number of Resource Group Configurations	2	2
Number of Policies	50	50
Number of Organizations	1	1
Is IdP on Premise or IaaS	None	None
Number of IdPs	0	0
Number of Shibboleth SPs to Shibboleth Applications	0	0
Number of Discovery Services for Shibboleth SPs	0	0
Number of SAML enabled Federation Targets (SPs)	0	0
Number of verified SFL enabled Federation Targets (SPs)	0	0
Number of non-verified SFL enabled Federation Targets (SPs)	0	0
Number of Attribute Management Processes	0	0
Number of On-Going Attribute Management Processes	0	0
Include Post Implementation Services	Yes	Yes
User Account Load	Custom	Custom
<b>Training</b>		
Basic Training	No	No
Advanced Training	No	No
Kiosk UI Training (Train the Trainer)	Yes	Yes
Pin Reset UI Training (Train the Trainer)	Yes	Yes
Help Desk UI Training (Train the Trainer)	Yes	Yes
Self Service Access Management UI Training (Train the Trainer)	Yes	Yes
HPAM UI Training (Train the Trainer)	No	No
Federation Configuration Training	No	No



VIRGINIA COMMONWEALTH UNIVERSITY  
**Federated Single Sign-On**  
**Full Time-Equivalent Student Pricing Model**  
**Pricing Valid Through 3/1/2017**

**Pricing Model:** FTE

(Additional Module Option  
 priced separately as requested)

**IdM Modules Required:**

- o Federated Single Sign-On

<b>Identity as a Service® Model (SaaS Subscription)</b>				
<i>(Based on above information. Initial Term: 5 Years)</i>				
<b>Annual Subscription Fee<sup>1,2</sup></b>	<b>Count</b>	<b>List</b>	<b>Discount</b>	<b>Net</b>
Federation: User Fee	28,456	\$40,976.64	50%	<b>\$20,488.32</b>
Federation: Base Fee	1	\$4,400.00	50%	<b>\$2,200.00</b>
<b>Total Annual Fees</b>		<b>\$45,376.64</b>		<b>\$22,688.32</b>
<b>Estimated Implementation Costs<sup>3</sup></b>	<b>Hours</b>	<b>List</b>	<b>Discount</b>	<b>Net</b>
Implementation Services	100	\$25,000.00	30%	\$17,500.00
<b>Total Year-1 Cost</b>				<b>\$40,188.32</b>

**Cost for Additional FTEs\***

One-time License: \$1.82  
 Annual IaaS® Subscription: \$0.72

\* New license prices are valid for three (3) years from the effective date of Agreement. Maintenance not included.



**VIRGINIA COMMONWEALTH UNIVERSITY**  
**Federated Single Sign-On**  
**Full Time-Equivalent Student Pricing Model**  
**Pricing Valid Through 3/1/2017**

**<sup>1</sup>FTE Pricing Notes:**

*Note: Users are calculated based on Student Full-time Equivalents (FTEs) numbers reported to IPEDS and not headcount for individual user types (e.g., student, faculty, staff, alumni, etc.)*

<b>Criteria</b>	<b>Description</b>
User License Fees	Student FTE only. Other Authorized user populations (students, faculty, staff, alumni, guests, etc.) are included without fee up to 10-times licensed Student
Connectivity License and Development Fees	No per-system connectivity or maintenance fees. New connectors developed without charge for up to 5 commercially-viable systems.
License Count Variance	5%: Student FTE count may exceed license count up to 5%.
Cost Increase "Resilience"	Excellent: No additional license/maint. fees related to growth in: <ul style="list-style-type: none"> <li>• non-FTE user populations</li> </ul>
License Administration	Simple: <ul style="list-style-type: none"> <li>• Only FTEs need be tracked.</li> </ul>

**<sup>2</sup>Connected Systems**

The implementation costs quoted herein assume that the systems below leverage existing Fischer connectivity or are commercially-viable and covered under the "Connected Systems" Terms below. The implementation costs presume the systems below leverage existing connectivity or are commercially-viable. AD,Banner,Oracle E-Directory,Google Apps,Blackboard,C-CURE,CBORD

Fischer's FTE Pricing Model includes connectivity and associated maintenance for systems within Fischer's connectivity library. If Fischer does not already have a connector for a commercially-viable system that is required by the institution, Fischer will develop it without charge for up to three (3) commercially viable systems (see definition below). Fischer reserves the right to charge for connectivity development and associated maintenance fees for connectors for any additional connectors. Connector fees for systems that are not commercially-viable for Fischer will be quoted separately. Software maintenance fees apply to all UNIQUE connectors in use and are valued at \$10,000.00 USD per unique connector.

NOTE: The development and maintenance fees for connectors is based on UNIQUE system (version/release), not per instance or connection point. For example, the cost basis for connecting to six (6) Oracle 11g Release 2: 11.2.0.1 databases is one (1) and not six (6).

NOTE: Commercially-viable" is defined as a COTS system that a reasonable number of other potential Fischer customers will need supported. The decision to waive development costs is made on a case-by-case basis and is based in part on projected or reported application market share and application version (e.g., application age, EOL, etc.).

**<sup>3</sup>Implementation Services Estimate & Assumptions**

Implementation services prices are for estimation purposes only and are not guaranteed. A formal quote for implementation services will be provided following a discovery workshop that commences upon contract execution. T&E are not included in estimate.

The implementation services in this quote are based on the following information:





**VIRGINIA COMMONWEALTH UNIVERSITY**  
**Federated Single Sign-On**  
**Full Time-Equivalent Student Pricing Model**  
**Pricing Valid Through 3/1/2017**

<b>Solution Requirements</b>	<b>On-Premise (N/A)</b>	<b>IaaS® (QTY)</b>
<b>Environment Specifics</b>		
Number of Environments	0	0
Additional HA Servers	0	0
Number of Global Identity Gateways	2	2
Number of MS Password Filters	0	0
<b>Modules</b>		
Password Management	No	No
Provisioning	No	No
HPAM	No	No
Federation	Yes	Yes
<b>Workshop Options</b>		
Password Management Workshop	No	No
Provisioning Workshop	No	No
HPAM Workshop	No	No
Federation Workshop	Yes	Yes
<b>Solution Specifics</b>		
Number of Initiation Points (Source of Authority)	1	1
Number of Password Management Targets	0	0
Number of Administrative Provisioning Targets	0	0
Number of Administrative Provisioning Workflows per target	0	0
Number of Automated Provisioning Target	0	0
Number of Automated Provisioning Workflows per target	0	0
Number of HPAM Account Types	0	0
Total Number of Unique Connected System Definitions	0	0
Number of Approval Configurations	0	0
Number of Selectable Resources	0	0
Number of Resource Group Configurations	0	0
Number of Policies	0	0
Number of Organizations	1	1
Is IdP on Premise or IaaS	On-Premise	IaaS
Number of IdPs	1	1
Number of Shibboleth SPs to Shibboleth Applications	0	0
Number of Discovery Services for Shibboleth SPs	0	0
Number of SAML enabled Federation Targets (SPs)	35	35
Number of verified SFL enabled Federation Targets (SPs)	0	0
Number of non-verified SFL enabled Federation Targets (SPs)	0	0
Number of Attribute Management Processes	0	0
Number of On-Going Attribute Management Processes	1	1
Include Post Implementation Services	Yes	Yes
User Account Load	No	No
<b>Training</b>		
Basic Training	No	No
Advanced Training	No	No
Kiosk UI Training (Train the Trainer)	No	No
Pin Reset UI Training (Train the Trainer)	No	No
Help Desk UI Training (Train the Trainer)	No	No
Self Service Access Management UI Training (Train the Trainer)	No	No
HPAM UI Training (Train the Trainer)	No	No
Federation Configuration Training	No	No

**SERVICE LEVEL TERMS AGREEMENT TERMS AND CONDITIONS  
FOR HOSTED IDENTITY AS A SERVICE® CLOUD DEPLOYMENTS**

**1. SERVICE AVAILABILITY**

Fischer uses its commercially reasonable efforts to make the Service available to authorized users twenty-four hours a day, seven days a week, or 100% of the time in each month, less the periods of time during which the Service is not available due to one or more of the following events (collectively, “Excusable Downtime”):

- 1.1. Routine Maintenance. Routine Maintenance means scheduled maintenance, Fischer’s notification policy is to announce the scheduled maintenance one month, two weeks, and one week in advance, but not less than 72 hours before the scheduled maintenance. Fischer will use its commercially reasonable efforts to schedule such maintenance during the weekend hours from 9:00 p.m. EST Friday to 3:00 a.m. EST Monday. Client will specify additional windows, known as “Critical Computing Days,” during which changes to the environment are not permitted with the exception of Unscheduled Maintenance as discussed in 8.6. These Critical Computing Days will be sent to Fischer no later than ninety (90) days prior to the occurrence;
- 1.2. Client Acts or Omissions. The acts or omissions of Client or Client’s employees, agents, contractors, vendors, or any end user or any other party gaining access to the Service by reason, directly or indirectly, of any act or omission of Client, including without limitation, the following:
  - a) Non-availability of Client’s connected systems or applications;
  - b) Non-availability of Client’s components for the Fischer Global Identity Gateway;
  - c) Upgrades or changes made to Client’s connected systems or applications without approval by Fischer and other changes made to Client’s connected systems or applications without reasonably sufficient time for Fischer to prepare for Client’s changes; and
  - d) Time waiting for an Authorized Client Representative to provide required information or to perform required actions.
- 1.3. Network Failures. A failure of the Internet and/or telecommunications networks external to those associated with the hosting data center; or
- 1.4. Force Majeure. The occurrence of any event that is beyond Fischer’s and the hosting data center’s reasonable control.
- 1.5. Test Environment. The Test Environment is excluded from the term "Service Availability" and the SLAs discussed herein do not apply, due to the nature of a test environment. Fischer will dedicate reasonable commercial efforts to ensure that the test environment will be available during the mutually agreed-to period.
- 1.6. Unscheduled Maintenance. Unscheduled maintenance that is performed on the Client’s solution and/or underlying infrastructure in response to a critical, unforeseen circumstance, such as a security vulnerability issue.

## **2. SERVICE LEVEL CREDITS**

- 2.1. Downtime. In the event Client experiences less than the target uptime of 100% (taking into account Excusable Downtime) for any given day, and a mutual determination in its reasonable judgment that such availability was caused by Fischer's failure to provide the Hosting Service (as defined in Section 8: Service Availability) and not due to other outages, Fischer shall credit Client's account the pro-rata fees for two (2) days of Hosting Service for each day the Hosting Service did not meet the target uptime of 100% (taking into account Excusable Downtime) provided that such credit shall not exceed 30 days per month. The service credit shall, in no event, exceed the Hosting Services fee attributable to the application one-month period. The service credit will be issues in the form of a credit memo for use against the next year's prepaid Hosting Services fees payable in the future for Hosting Services. As a condition precedent to Client obtaining a service credit, Client must request, in writing, the service credit attributable to a particular month within thirty (30) days following the last day of such month. Service credits shall be deemed to be a form of liquidated damages, and Client acknowledges and agrees that such do not operate by way of penalty and constitute a genuine attempt to pre-estimate loss.
  
- 2.2. Termination for Chronic Problems. Client shall have the right to terminate the Hosting Services in the event that Fischer fails to achieve the target uptime of 100% for a month (taking into account Excusable Downtime) for three (3) consecutive months or three (3) months in six (6) month period. To terminate under this section, Client must provide Fischer with written notice of termination within thirty (30) days of the chronic problems occurring, and such termination will be effective thirty (30) days following Fischer's receipt of such written notice. In the event of termination under this section, Fischer will provide professional services at the discounted hourly rate specified above and with no additional charges or fees to migrate Client's installation to an on-premise installation.

## **3. CHANGES TO THE SERVICE**

- 3.1. Fischer reserves the right to make modifications, changes, updates and upgrades to the Service and the manner in which Fischer provides the Service (including the Fischer-maintained operating environment from time to time). Fischer shall use its commercially reasonable efforts to minimize any disruption to the Service caused by such modifications, changes, updates and upgrades. Any such modifications, changes, updates and upgrades shall not waive Fischer's obligations under any other provisions of this Agreement.
  
- 3.2. The rules and procedures related to notifying the Client of such changes are applicable under this clause. For software upgrades (including new versions, service packs and hot fixes), the Client is notified up to 60 days in advance prior to said upgrades. The timing

of upgrading the test environment can be mutually agreed upon by both parties for convenience. The procedure for changes to the service (platform and underlying Fischer software) is as follows:

- i. The assigned technical account manager will notify the customer of an upgrade to the test platform;
- ii. The test platform will be upgraded and the Client will be given time to test the new version against their existing solution. At the request of the client, a Provider technician can be made available to aid in testing, as well as to answer any questions about new features and functionality introduced. The Client will be notified by the Account Manager of such upgrades and the Client is encouraged to request support for testing service changes.
- iii. The Client will provide the authorization (including date and time where reasonably applicable and as long as the service change is not related to a discovered security vulnerability) to upgrade or apply said changes to the production platform.

Changes made to the solution running under the service are governed by the change control processes authorized by Fischer executive management. Upon request, Fischer can provide the Client with the official change control document as it pertains to changing the service / solution.

## HOSTING SERVICE SUPPORT

### A. Scope

**This describes the Support provided by Fischer as part of an Identity as a Service® deployment.**

Any terms and conditions in herein that do not pertain solely to the Service infrastructure and maintenance, Fischer Identity™ operational maintenance, or solution administration (services) do not apply. Product support related to Fischer Identity™ software is governed by the Client’s Master Software License Agreement.

### B. Definitions

The following terms shall have the respective meanings given below as used in this document.

1. “Error” means one or more reproducible failures of the Service to substantially comply with the User Guide or the occurrence of Service down time which is not due to Excusable Downtime as stated herein.
2. “Fix” means the repair or replacement of object or executable code versions of Fischer Software included as part of the Service to remedy an Error.
3. “Workaround” means a change in the procedures followed or that you supply to avoid an Error without impairing your use of the Service.
4. **“Response Time” means the interval from when Fischer receives a Support Request from Client to the time that Fischer responds to the Authorized Client Representative for the initial conversation.**
5. “Solution Modules” mean the major capabilities or components of the Service that can be individually licensed. For organizations licensing the entire suite, the modules are Automated Role & Account Management, Password Reset & Synchronization, Privileged Account Access and Identity Compliance. Sub-modules count as modules only when they are individually licensed outside the suite: Access Termination and Role & Account Management.
6. **“Support Request” means a request for support to Fix or provide a Workaround for an Error in the Service or a request for support that involves no modifications to the Service, such as a question.**

### C. Levels of Support

Fischer Technical Support is Client’s point of contact for any support services provided by Fischer hereunder.

Support Level	Description
Level 1	<p>This is the initial support level responsible for Support Requests and Work Orders for Professional Services. Level 1 representatives receive support calls, and in consultation with the Authorized Client Representative, determines the initial Priority Level for the Support Request. A Level 3 representative may modify the Priority Level of a Support Request if such representative determines that the Support Request has been assigned the wrong Priority Level. Sample Level 1 activities include but are not limited to:</p> <ul style="list-style-type: none"><li>• Being the point of contact for Authorized Client Representatives related to all software issues and changes (bugs, usability questions and enhancements).</li><li>• Collaborating with an Authorized Client Representatives to establish the priority of support requests.</li><li>• Answering questions about the functionality of the software.</li><li>• Performing initial troubleshooting and providing known, documented fixes or workarounds when available.</li><li>• Recording support requests, opening support tickets and assigning ticket numbers</li><li>• Tracking the status of support tickets.</li></ul>

	<ul style="list-style-type: none"> <li>• Transitioning support requests to Level-2 Technical Support when required.</li> <li>• Communicating problem resolution to Authorized Client Representatives.</li> </ul>
Level 2	<p>Level 2 Support: This is a more in-depth technical support level than Level 1 containing more knowledgeable personnel experienced at administrative level support. Technicians in this realm of knowledge are responsible for assisting Level 1 personnel to solve basic technical problems and for investigating elevated issues by confirming the validity of the problem and seeking for known solutions related to these more complex issues. A key responsibility of this level is to determine whether the problem is part of the “solution,” i.e., the configuration and workflows, or if the problem is caused by an underlying software issue. All configuration and workflow issues should be solved at this level. Sample Level 2 activities include but are not limited to:</p> <ul style="list-style-type: none"> <li>• Conducting root-cause analysis to determine whether a problem is caused by the configuration or by an underlying software issue.</li> <li>• Transitioning problems to the appropriate Level-3 Technical Lead as required via the terms stated in Section V SUPPORT REQUESTS AND PRIORITY LEVELS.</li> <li>• Communicating problem resolution to Authorized Client Representatives.</li> </ul>
Level 3	<p>Level 3 Support: Level 3 support will be provided related to Software Errors only. Level 3 support is synonymous with Development as the issues coming to this level typically require software fixes and may require temporary workarounds if an error cannot be solved rapidly. Although the vast majority of “solution” problems should be identified and corrected by Level 2 technicians, Level 3 is available to assist Level 2 in determining whether a problem is related to the solution or to the software. Sample Level 3 duties include but are not limited to:</p> <ul style="list-style-type: none"> <li>• Leading the programming and quality assurance efforts for any coding and testing required to resolve software problems.</li> <li>• Delivering workarounds for software errors that cannot be resolved rapidly.</li> <li>• Communicate problem resolution to Level-2 Specialists.</li> </ul> <p>*Note: Time spent by Fischer on L3 support requests that are determined to NOT be related to a software error will be billed to the Client. No solution customization services of any kind are included in Level 3.</p>

#### D. Support Requests and Priority Levels

1. Requesting Technical Support. Fischer recommends that Client first refer to the documentation, User Guide and any on-line help provided by Fischer for possible solutions to problems prior to issuing a Support Request. Client may request support via the following methods:

- Web: Fischer Online Customer Support Portal
- Telephone: +1 239-436-2700
- Email: support@fischerinternational.com

2. Technical Support Hours. If Client continues to experience an Error with the Service, an Authorized Client Representative must issue a Support Request. Support Requests may be submitted seven days a week, 24 hours a day, except during periods of maintenance or force majeure. Each Support Request will be handled in the manner described in Section C above.

3. Factors Used to Determine Priority Levels. The following characteristics are used by the Level 1 Fischer support representative, in consultation with Client, to identify the Priority Level of an Error submitted through a Support Request: (a) business and financial exposure and impact; (b) work outages; (c) the number of Covered Persons affected; (d) when the functionality is required; and (e) whether a Workaround is available. It is not necessary (nor is it likely) to have a perfect match of each characteristic to categorize a reported Error at a particular Priority Level. Each reported Error will be weighed against

each of the characteristics to make an overall assessment of which Priority Level best describes the reported Error.

## Priority Levels

Priority 1 (Critical)	Priority 2 (High)	Priority 3 (Medium)	Priority 4 (Low)
<b>Business and financial exposure</b>			
The Error creates a serious business and financial exposure for Client.	The Error creates a substantial business and financial exposure for Client.	The Error creates low or little business and financial exposure for Client.	The Error creates minimal business and financial exposure for Client.
<b>Work Outage</b>			
The Error prevents Client from completely utilizing the Service to perform critical work and a majority of Client's business operations are affected.	The Error prevents Client from utilizing material portions of the Service and affects a substantial portion of the Client's operations.	The Error prevents Client from utilizing some substantial features of the Service and affects a significant portion of the Client's operations, but Client is still able to complete most other tasks.	The Error prevents Client from utilizing some non-substantial portion of the Service, but Client's operations are not materially affected and Client is able to complete most other tasks.
<b>Number of Covered Persons Affected</b>			
The problem affects a majority of Client's Covered Persons.	The problem affects a substantial proportion of Client's Covered Persons.	The problem affects a small number of Client's Covered Persons.	The problem only affects a minimum number of Client's Covered Persons.
<b>Timing of Usage</b>			
The failed function(s) are currently required.	The failed function(s) are currently required.	The failed function(s) will be required within two weeks.	The failed function(s) are not required for more than two weeks.
<b>Workaround</b> [Note, this bullet carries the heaviest weighting of the characteristics for Priority 1 and 2.]			
There is no Workaround to the Error (i.e., the job cannot be performed in any other way).	There may or may not be a Workaround to the Error. (i.e., the job may not be performed in some other way)	There is likely a Workaround to the Error.	A workaround for the Error is available and can be implemented (i.e., the job can be performed in some other way).
<b>Response Time to Conduct Initial Conversation</b>			
Within two hours	Within four hours	By next (U.S.) business day	Within one weeks

### 4. Service Levels.

The levels of service provided by Fischer to Client are described below.

Priority 1 Support Requests: Fischer technical support personnel work around the clock until the problem is resolved. It is critical that an Authorized Client Representative is available to provide information and to perform actions as required to resolve the Error, or Fischer is permitted to automatically lower the Priority Level of the Support Request to Priority 2.

Priority 2 Support Requests: at least one Fischer technical support person is assigned to address the



problem during normal business hours. During this time, an Authorized Client Representative is required to be available to provide information and to perform actions to resolve the Error, or Fischer is permitted to automatically lower the Priority Level of the Support Request to Priority 3.

Priority 3 and Priority 4 Support Requests: Fischer will schedule work as appropriate. Resolution may be provided in the next scheduled product release.

Support Requests are automatically escalated to higher levels within Fischer as provided in the table below.

**Fischer Escalation for Support Requests**

<b>Priority</b>	<b>Criteria for Escalation Within Fischer</b>	<b>Notification to</b>
<b>Priority 1 (Critical)</b>	Every 2 hours from time of creation or last update	1. Director of Operations 2. Support Manager 3. Primary Support Specialist
<b>Priority 2 (High)</b>	Every 4 hours from time of creation or last update	1. Support Manager 2. Primary Support Specialist
<b>Priority 3 (Medium)</b>	No Response to Client (which may include plans for a Workaround or a Fix in the next release) has been communicated to Client within in 1 business day.	1. Support Manager 2. Primary Support Specialist
<b>Priority 4 (Low)</b>	No Response to Client (which may include plans for a Workaround or a Fix in the next release) has been communicated to Client within 1 week.	1. Support Manager 2. Primary Support Specialist

**5. Client Responsibilities.**

- a) Prior to initiating a Support Request, the Authorized Client Representatives will attempt to resolve the issue by consulting any on-line help provided by Fischer.
- b) The Client will report all suspected Errors through the Authorized Client Representatives to the Fischer Support staff. Client end users and Covered Persons may not contact Fischer support resources directly to report a problem or Error. Reports will include the minimum required information sufficient for Fischer to reproduce the suspected Error. Fischer strongly encourages Client to report Priority 1 and Priority 2 support requests by telephone to expedite resolution. By default, support requests received through e-forms, fax, or email messages are initially treated as Priority-3 Support Requests and are responded to within 1 business day.
- c) An Authorized Client Representative is often required to provide information or perform actions so that Fischer can provide support services. The Client will use reasonable effort to provide required information in a timely manner using the same schedule as outline in Section 4.
- d) In certain situations, detailed information regarding the Client’s system environment may be necessary to affect a timely resolution. In these situations, and other integration/gateway related issues, Fischer may require the involvement of the Client’s IT resources to provide information necessary to assist in Error or problem resolution.
- e) Client must specify whether changes required to resolve a Support Request or to implement a Work Order must be approved by Client before being enacted.
- f) The Client is responsible for properly maintaining the functional operation of its IT equipment and interfaces, including connectivity to the Internet. Consulting, implementation, integration, support for Client Interfaces, and training services that may be needed for the Client to take

advantage of Service revisions or Updates are not within the scope of the support provided pursuant to this document.

- g) Prior to logging any connectivity problems, the Client will verify that they are able to reach other popular Internet sites such as Google (<http://www.google.com>).
- h) The Client is responsible for virus protection for Client workstations and all of the Client's host systems that are networked to those workstations or the Service.
- i) The Client must use Firefox 3.6 or higher, Safari 5 or higher, Google Chrome, Microsoft Internet Explorer 7.0 or higher (Internet Explorer 9 is supported in compatibility mode in Fischer Identity™ V4.2), as such requirement may be reasonably updated during the Term by Fischer upon reasonable advance notice to Client.
- j) The Client is responsible for configuration of its corporate Internet firewall to allow any necessary ports to be used.
- k) The Authorized Client Representatives will not share their login identifier or password.

The above responsibilities in no way waive the hosting obligations of Fischer as set forth under other provisions of this Agreement.

6. Connector Version Support Policy.

- a) Connectors are supported for the version and release of the connected system for which they are delivered and for the version and release of the Fischer Software for which they are delivered.

# References for RFP

## Virginia Commonwealth University

### Identity and Access Management System

Refer to question PS-APP-007.

The information below is CONFIDENTIAL.

Customer: University of Maryland, University College

Contact: Joanna Days, Office of Information Technology

Location: Adelphi, MD

Phone: (301) 985-7181

Email: joanna.days@umuc.edu

Years Serviced: 2

User Base: Enrollment 60,000 FTES. Licenses: 600,000.

Customer: Howard Community College

Contact: Michael Heinmuller, Director, User and Network Services

Location: Columbia, MD

Phone: mheinmuller@howardcc.edu

Email: (443) 518-4910

Years Serviced: 4

User Base: Enrollment: 6,200; Total licenses: 68,200

Customer: Pepperdine University

Contact: Kevin Phan, Associate CIO

Location: Malibu, CA

Phone: (310) 506-4373

Email: kevin.phan@pepperdine.edu

Years Serviced: 3

User Base: Enrollment: 6,200; Total licenses: 68,200

Customer: Maryland Institute College of Art

Contact: Susan Miltenberger, AVP of Technology Systems & Services

Location: Baltimore, MD

Phone: 410/225-2562

Email: smiltenb@mica.edu

Years Serviced: 5

User Base: Enrollment: 2,200; 24,200 total licenses

Customer: Frostburg State University

Contact: Troy Donoway, CIO

Location: Frostburg, MD

Phone: 301.687.7003

Email: dtdonoway@frostburg.edu

Years Serviced: 4

User Base: Enrollment: 5,756; 95,240 total licenses

CONFIDENTIAL



# CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY) 11/14/2016
---------------------------------

**THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.**

**IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).**

<b>PRODUCER</b> Lassiter-Ware Insurance of Maitland 2701 Maitland Center Parkway Suite 125 Maitland FL 32751	<b>CONTACT NAME:</b> Bekah Pickering <b>PHONE (A/C, No. Ext):</b> (800)845-8437 <b>FAX (A/C, No):</b> (888)883-8680 <b>E-MAIL ADDRESS:</b> BekahP@lassiter-ware.com																					
<b>INSURED</b> Fischer International Systems Corporation, et al P O Box 9107 Naples FL 34101-9107	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th colspan="2" style="text-align: center;">INSURER(S) AFFORDING COVERAGE</th> <th style="text-align: center;">NAIC #</th> </tr> <tr> <td>INSURER A:</td> <td>Pacific Indemnity Company</td> <td style="text-align: center;">20346</td> </tr> <tr> <td>INSURER B:</td> <td>Federal Insurance Company</td> <td style="text-align: center;">20281</td> </tr> <tr> <td>INSURER C:</td> <td>AXIS Surplus Insurance Co.</td> <td style="text-align: center;">26620</td> </tr> <tr> <td>INSURER D:</td> <td></td> <td></td> </tr> <tr> <td>INSURER E:</td> <td></td> <td></td> </tr> <tr> <td>INSURER F:</td> <td></td> <td></td> </tr> </table>	INSURER(S) AFFORDING COVERAGE		NAIC #	INSURER A:	Pacific Indemnity Company	20346	INSURER B:	Federal Insurance Company	20281	INSURER C:	AXIS Surplus Insurance Co.	26620	INSURER D:			INSURER E:			INSURER F:		
INSURER(S) AFFORDING COVERAGE		NAIC #																				
INSURER A:	Pacific Indemnity Company	20346																				
INSURER B:	Federal Insurance Company	20281																				
INSURER C:	AXIS Surplus Insurance Co.	26620																				
INSURER D:																						
INSURER E:																						
INSURER F:																						

**COVERAGES** **CERTIFICATE NUMBER: 16/17 FISC MASTER w/** **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	<input checked="" type="checkbox"/> <b>COMMERCIAL GENERAL LIABILITY</b> <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR  GEN'L AGGREGATE LIMIT APPLIES PER: <input checked="" type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input type="checkbox"/> LOC OTHER:			35768315ECE	3/1/2016	3/1/2017	EACH OCCURRENCE \$ 1,000,000 DAMAGE TO RENTED PREMISES (Ea occurrence) \$ 1,000,000 MED EXP (Any one person) \$ 10,000 PERSONAL & ADV INJURY \$ 1,000,000 GENERAL AGGREGATE \$ 2,000,000 PRODUCTS - COMP/OP AGG \$ 2,000,000 \$
B	<b>AUTOMOBILE LIABILITY</b> <input type="checkbox"/> ANY AUTO <input type="checkbox"/> ALL OWNED AUTOS <input checked="" type="checkbox"/> HIRED AUTOS <input type="checkbox"/> SCHEDULED AUTOS <input checked="" type="checkbox"/> NON-OWNED AUTOS			73508370	3/1/2016	3/1/2017	COMBINED SINGLE LIMIT (Ea accident) \$ 1,000,000 BODILY INJURY (Per person) \$ BODILY INJURY (Per accident) \$ PROPERTY DAMAGE (Per accident) \$ \$
B	<input checked="" type="checkbox"/> <b>UMBRELLA LIAB</b> <input checked="" type="checkbox"/> OCCUR <input type="checkbox"/> <b>EXCESS LIAB</b> <input type="checkbox"/> CLAIMS-MADE DED RETENTION \$			79794090	3/1/2016	3/1/2017	EACH OCCURRENCE \$ 10,000,000 AGGREGATE \$ 10,000,000 \$
	<b>WORKERS COMPENSATION AND EMPLOYERS' LIABILITY</b> ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	Y/N	N/A				<input type="checkbox"/> PER STATUTE <input type="checkbox"/> OTH-ER E.L. EACH ACCIDENT \$ E.L. DISEASE - EA EMPLOYEE \$ E.L. DISEASE - POLICY LIMIT \$
C	<b>Tech &amp; Prof Liab w/ Content Security &amp; Privacy Liab</b>			ECN000227161601	3/1/2016	3/1/2017	Each Wrongful Act \$2,000,000 Total Limit of Insurance \$2,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

<b>CERTIFICATE HOLDER</b>  Virginia Commonwealth University RFP #7216216JC Attention: Jackie Colbert 912 W Grace St. 5th floor Richmond, VA 23284	<b>CANCELLATION</b>  SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.  AUTHORIZED REPRESENTATIVE  Paul Ziccardi/REBEKP
--	--

Fischer International  
Technical Requirements/Questions  
June 21, 2017

**Roadmap:**

1. You indicated that at the current time, Fischer does not have the capability to check whether an external event (e.g. Training completion in a LMS) occurred before proceeding with provisioning or de-provisioning workflow. Are there any plans of integrating this capability in the future? If so, when?

***[Fischer] We can add functionality as needed. The context that was discussed was introducing training completion lookups during an approval process, and to release the event only when training has been completed. This is where an enhancement may be applicable.***

***As discussed, Fischer can provide some of this functionality today. We can schedule a process to look at the field holding the training completion flag. That way, the provisioning process would initiate only after training completion flag is set. So, an enhancement may or may not be required to our product, depending on how we design the process. If an enhancement is required, Fischer will build it during the deployment.***

2. When will responsive design be built into the user interface?

***[Fischer] The current target is to have something completed in 2018. I know this is a broad response, but our feature set is very extensive and we will make sure, as we move to a responsive framework, we do it correctly. We will be officially kicking off this component of our roadmap in the next 4 weeks. It will take some time to finish properly while still maintaining continuity for our existing and new customers. It will be our number one priority.***

**Narrative:**

3. Submit a narrative on how you would recommend the provisioning and setup of IAM with regards to our teaching hospital. A methodology in very general terms.

***[Fischer] The assumption is the teaching hospital is somewhat secluded from the rest of the VCU infrastructure. If this is in fact the case, Fischer simply needs to place our Global Identity Gateway ("GIG") inside the teaching hospital's network. The GIG is placed inside the firewall and we will work together on SSL / port requirements to ensure Fischer can***

***communicate (and provision) identities inside the teaching hospital. You will need a minimum of two (2) distinct GIGs for high availability. These can be on virtual or physical servers. For GIGs, Fischer can handle load balancing via the feature we have in the product called "GIG clustering". At this point, Fischer is able to provision to the teaching hospital as required by the overall access control model for VCU.***

4. Provide a narrative with regards to ABNEs - methodology and example of how other school address the provisioning process for potential students and the de-provisioning process for those who elect not to attend VCU.

***[Fischer] Provision with a preset end date and delete if they don't "claim" in a certain amount of time. Timer can be Fischer side or client side. In Addition Clients should have a "timer" on their side if an applicant doesn't change status in X amount of time they get dropped from the SOA which spawns a Deprov event. The appropriate management of usernames will be determined during the Professional Services engagement.***

5. Submit a narrative in regards to integration with BEIS (Banner Enterprise Identity Service) for real time updates and a batch (pull/push) updates. Discuss the pros and cons of having a hybrid BEIS and batch configuration for data updates from Banner.

***[Fischer] We typically do not recommend organizations use BEIS because of the amount of irrelevant data and transactions that are introduced to our software, which eats up computing power unnecessarily. With that being our opinion, we do support BEIS and have it deployed in production and we are capable of integrating with BEIS.***

***The pros of using BIES in conjunction with a batch configuration is most likely only a pro if that is the way your infrastructure is currently built. We can support this model, and that is a pro.***

***The cons of this model will really lie in what is coming through BEIS and what is coming through the batch process. We would have questions such as: (1) Do we have to merge the data first, before creating an identity? (2) Will a complete "identity record" be passed from each source of authority, therefore creating two distinct SoAs? If these are two distinct SoAs, this is a pro, if we need to merge the data sets, we will need further discussions to ensure we properly merge the attributes and validate we have a complete identity record before we attempt to evaluate and provision. In addition, we have seen other customers have a difficult time implementing BEIS.***

**Requirements:**

Provide a Yes or No response to each bullet in the Requirements section. If the response is No, include any explanation or alternative method.

**Duplicate Account Matching:**

6. Clear ability to easily view and troubleshoot duplicate accounts that have been created in error. If possible, ability to flag these duplicate accounts automatically before they are ever provided to customers so that a review can be made to ensure that these duplicate accounts are merged before the customer even knowing of their account.

***[Fischer] Yes, this is supported.***

**Help Desk Tools:**

Our help desk technicians need to have the capability for the following help desk tools in order to provide adequate password and account management support:

7. An interface where help desk personnel can view and search critical identity attributes, such as name (first, last, surname, username), account IDs/usernames, ID card information, title, department/school, MBU, affiliation, SSN and DOB information, email forwarding information, password policy information, login and intruder lockout information, etc.

***[Fischer] Yes, this is supported.***

8. Would like to have the ability to restrict specific data fields and give specific data fields view/edit access depending on help desk personnel role.

***[Fischer] Yes, this is supported.***

9. A password management tool which allows help desk personnel to either set a temp password, or push a notification to a customer's MFA option (so they can reset on their own), clear grace logins, unlock accounts, add and remove special/notes descriptions to accounts, clear login expirations, and enable/disable accounts to perform basic password management for those customers calling for advanced support.

***[Fischer] Yes both methods are supported (temp password or forcing the user to "reclaim" their account. Comments could be captured at that time.***

10. Ability to update MFA information for users who are contacting the office for support (i.e. update a listed phone number, alternate email address, etc. in case a customer has out of date information stored).



***[Fischer] Yes, this is supported.***

11. Ability to track following information on accounts for troubleshooting compromised account situations: IP address information on location where account was last reset, who reset the password (was it account owner reset, or reset by help desk personnel), full account audits so that all account events are tracked and easily viewable by help desk personnel.

***[Fischer] Yes, this information is tracked and can be reviewed in a report.***

12. Audit records on help desk personnel actions such as what account was viewed/edited, what action took place, and by whom.

***[Fischer] Yes, the actions taken by the help desk personnel is tracked and is available to review.***

13. Interface where help desk personnel are able to view all access that a user account has to different applications/systems to troubleshoot whether or not someone has access to the application/system they are contacting us for support.

***[Fischer] Yes, this is supported.***

#### **Self Service Password Management:**

14. Our customers need to have the ability to completely manage their account in a self service fashion throughout the entire account lifecycle, from account creation through their time at VCU, all the way to when they have left the university and are now "former" with access to limited resources. True self service password management needs to include the following capabilities with the new IAM product:
15. Self service online account claiming where the customer must input their MFA options upon first time setup of their user account.

***[Fischer] Yes, we can meet this requirement, by requiring the user to update their profile (MFA attributes) the first time they set their password.***

16. Ability for customers to easily manage their MFA options online after initial setup of their account.

***[Fischer] Yes, this is supported.***

17. Ability for customers to reset their account password using a self service portal and multiple MFA options (SMS, email, DUO, challenge questions, etc.) so that a customer no longer has to contact the help desk to do any type of password reset.

***[Fischer] Yes, this is supported.***

18. Ability to manage their password via computer, as well as on mobile devices (and able to connect to these tools from off campus connections).

***[Fischer] Yes, this is supported.***

19. Ability for those who have left the university to easily reactivate their account access online by providing MFA information (instead of forcing these individuals to contact the help desk to re-enable their account which is the current method we use).

***[Fischer] Yes, upon log in, Fischer can setup a process to enable their account.***

#### **Connectors:**

List of all connectors that will be included:

20. Must have connectors: Active Directory, LDAP, eDirectory, Google Apps (G Suit), Blackboard, CBord suite, Banner, JDBC, Delimited File, REST

***[Fischer] Yes, all connectors listed are included. All are out of the box with the exception of CBord suite which will be integrated leveraging a flat file***  
**Fisher includes an extensive connector library at no additional cost to customers. Each customer has access to all the connectors in the library, including those connectors that the institution may not be implementing as part of the initial project. If the institution adds additional systems in later phases of the project or in subsequent SOW's, those connectors are still available at no additional cost.**

**Additional content discussed during the June 15<sup>th</sup>, 2017 onsite meeting: Fischer does not charge for updates or upgrades. Unless an update or an upgrade event results in the addition or modification of solution components, there will never be associated charges.**

**Fischer allows for institutions to migrate from one delivery methodology to another (On premise to hosted) or from one licensing methodology to another (FTE to Headcount).**

**When migrating from an on premise to solution to a hosted solution, the only associated services charges would be related to the provisioning of**

**the actual infrastructure components – there are no other services cost involved. There are additional license conversions that will be covered in the conversion matrix outlined in the Fischer agreement, credit is given for previously paid OTP licenses and annual maintenance.**

**When migrating license methodology there is a onetime administrative fee of \$1000.00. In addition, any delta in licensing costs related to the license modification would be invoiced accordingly.**

**Business, Terms, and Conditions Questions:**

21. The commitment for the utilization of SWaM businesses certified by the Virginia Department of Small Business and Supplier Diversity (DSBSD) is one of the evaluation criteria that determines the award of the contract. VCU has a 42.0% SWaM annual expenditure goal. What percentage of the potential contract can your firm subcontract with Virginia certified SWaM's businesses?

***[Fischer] Fischer has worked with a number of reselling partners that qualify as a SWAM entity, and the intent is for Fischer to bill all licensing costs through a SWaM vendor (Attronica), representing more than the 42% of the total contract value in order to satisfy the requirements of Appendix I represented in the RFP.***

22. Please confirm how long after a contract award can your firm commit to dedicating resources for the VCU project and begin to provide the contract products and services.

***[Fischer] Upon execution of the contract, Fischer can engage immediately to discuss logistic, timing, pre-requisites and overall staffing and technical requirements to kick the project off. This meeting is typically at the project sponsor / Fischer executive level. Once we've level set dates, timing and expectations we can typically engage within 4-6 weeks. During this 4-6 week period, our customers are actively working to provide use the necessary information to begin discover / design. Fischer can engage during this 4-6 week period on a periodic basis to ensure our customer is able to progress and move towards the kickoff meeting. During the kickoff, we like to discuss when and how components can be delivered and the project plan, including milestones as well.***

23. Provide an implementation schedule for the delivery and installation of the system for use at VCU.

***[Fischer] On average, our deployment model will allow for 4-6 weeks for discovery (pre-SOW), 1-2 weeks for product installation and infrastructure design, 1-2 weeks for password management, 6 weeks for provisioning, 2***

**weeks for self-service, and 2 weeks for production migration. Please reference the Implementation Methodology document that was included in the Fischer RFP response for additional clarification.**

24. Your firm agreed to accept the Procurement Requirements in Section V.C of the RFP. Confirm that consistent with agreement of these terms that travel and living expenses are included in the fixed fee for the IAM solution and implementation.

***[Fischer] In the new Services quote to be provided based on the bullet item below, the travel costs will be incorporated into the Fixed Fee implementation costs***

25. Your firm agreed to accept the RFP terms and conditions to govern any resulting contract. In the Special Terms and Conditions, any price increase at the time of renewal cannot increase by more than the All Items category of the CPI-W (Table 6) of the CPI for the latest twelve months for which statistics are available. In your proposal there is some conflicting information about a cap on price increases at the time of renewal. Confirm agreement with the cap on price increases at the time of renewal in the RFP Special Terms and Conditions.

***[Fischer] Fischer will adopt and incorporate the annual increase language represented in the VCU RFP Section (O) sub (1) into all agreements, licenses, statements of work, or other instruments related to the contract. Fischer will conform to the VCU standard annual renewal form when issued or applicable.***

26. What is the discount offered on the prices proposed for the IAM solution?

***[Fischer] Fischer Identity offers Higher Education clients our most aggressive pricing including a 50% discount on software and 30% discount on Professional Services***

27. Submit a price list with the prices discounted with the offered price reduction percentage from list price for other potential users of the contract. Include prices for software (perpetual, subscription (SaaS), hybrid), implementation, and training. Include prices for both FTE and Headcount.

***[Fischer] VASCUPP community pricing provided for your review***

28. VCU wants to contract for an on-premises IAM solution. Please review the price offer and resubmit a revised Pricing Schedule for a VCU on-premises IAM solution to include license cost for the FTE Model, annual maintenance, training, and implementation costs with travel and living expenses incorporated on a firm, fixed price basis.

***[Fischer] Fischer has provided an updated for an on premise deployment that includes training and travel costs incorporated into the Services quote***

29. Is the pricing offered the most favorable pricing offered to any customer for the same volume at this particular time? What additional discounts or price breaks can be offered for this contract without changing any of the project approach and deliverables proposed? Include any price reductions offered in the revised Pricing Schedule for any lower unit prices and deeper discounts.

***[Fischer] Fischer has provided an updated price quote that includes a VASCUPP additional discount***

30. Confirm that the Clarification Response dated January 25, 2017 is incorporated into the Negotiation Response by reference.

***[Fischer] Clarification questions to RFP # 7216216 dated January 25, 2017 are incorporated into Negotiation Response.***



Clarification Questions for RFP #7216216JC

1. Does all attribute data need to be in a central identity datastore? Can it be retrieved on-demand from an external datastore if the data is not currently in the datastore or is sensitive in nature?

Fischer only needs to store information necessary for user qualifications or displaying in the user facing UIs, such as user type, user status, first name, last name, etc. Other information can be retrieved, on-demand, from an external datastore as needed.

2. What platforms are needed and what is the quantity of platforms needed to implement the proposed solution?

Fischer is system agnostic, meaning an on-premise deployment can be installed on a UNIX or Windows Server. We support MSSQL, Postgres and Oracle Databases for the Fischer datastore. The solution also requires an LDAP for authenticating into the Fischer product. The solution can be installed in a High Availability mode. Separate instances will be needed for production and test environment. 2 servers will be used for each instance (3 if using SSO). Please refer to the Official Pre-Requisites Guide for more details.

For cloud deployments Fischer Identity requires the customer install a Global Identity Gateway (GIG) to enable security communication between the cloud and the customers network. The GIG may be installed in a clustered mode. Separate GIG instances will be needed for production and test environments. Each data center hosting systems being managed by Fischer will need to have a GIG or GIG Cluster installed in it. Please refer to the Official Pre-Requisites Guide for more details.

3. Provide details on your experiences with BEIS:

- How it was used

Fischer offers an SPML listener that is leveraged to communicate with Banner and introduce events to the identity suite. This information is processed immediately upon receipt.

- Creating initial identity record?

BEIS will send the PIDM to Fischer which will ensure that Fischer maintains the correct users identity record.

- Frequency of updates



Updates are received in real-time. Fischer processed the request as soon as they are received from the SPML listener.

- Problems, challenges

Some customers do not want to deploy BEIS or maintain the solution as a 3rd party between the SoA and Fischer. There is a risk that BEIS will not work correctly / stop working and transactions could be lost (at no fault of Fischer). Customers may choose to use a near real-time feed to eliminate these risks.

#### 4. Banner Integration Questions:

- Provide details on your experience with Banner (Adapters other than BEIS, other methods)

Fischer provides JDBC connectivity to the Oracle database and we typically work with our customers to export SoA data via defined views.

- Does your proposal allow for a second authoritative source other than Banner? (Provide details on how that is supported)

Fischer can pull from one or multiple authoritative sources. Fischer can set up real-time (where available) or near real-time pulls from multiple sources. This data is processed and stored in a central staging area. From the staging area the requests are sent to Fischer's provisioning engine to evaluate the user for their qualifying roles.

#### 5. The following questions are about creation of a unique identity:

- Can your system create the unique identity?

Fischer can be tasked with generating the unique identity for a user such as email, login id, user name, etc. Fischer can also be tasked with creating a unique identifier for users that are not coming from Banner, such as contractors, guests, temps, etc.

- Describe the process and options.

This process can be built using your business logic and error handling would be implemented to verify uniqueness before the unique identity is used. When Fischer creates a user name, it will verify that the name is unique against one or many targets. This will ensure that the user name is unique not only in the target system but also in any other system. Fischer can also check for uniqueness in external systems, such a repository of known user names that should never be used.

- What attributes of the entity are used to determine uniqueness, SSN, Name, Birthdate...?



Fischer can be configured to check any number of attributes to determine uniqueness. This is not limited to SSN, Name and Birthdate. Any information retrieved from the SoA can be used during this process. This can be done upfront upon receiving the information from one of the SoAs or can be done by the Fischer product using our User Matching feature. This feature can check against incoming attributes and compare them to existing users in Fischer. If a match is found authorized user will be alerted to take action on the account. They will have the ability to merge the identities or create a new identity. Exact matches can also be managed automatically.

FISCHER INTERNATIONAL IDENTITY, LLC

By:

A handwritten signature in black ink, appearing to read "R. Andrew Sroka", written over a horizontal line.

R. Andrew Sroka, President & CEO