

University of California (UC)

Contract # 2021003140

for

IT Security Tools

Identity Management (Category 3)

with

Fisher Identity LLC

Effective: September 29, 2021

The following documents comprise the executed contract between the University of California, Office of the President and Fischer Identity, LLC effective September 29, 2021:

- I. Executed Purchasing Agreement
- II. Supplier's Response to the RFP, incorporated by reference.



UNIVERSITY OF CALIFORNIA

Purchasing Agreement # 2021003140

The Agreement to furnish certain cloud computing services described herein and, in the documents, referenced herein (“Goods and/ or Services”), is made by and between The Regents of the University of California, a California public corporation (“UC”) on behalf of the University of California, and **Fischer Identity LLC**. (“Supplier”). This Agreement is binding only if it is negotiated and executed by an authorized representative with the proper delegation of authority.

The terms and conditions of this Agreement will supersede and take precedence over those of any pre-existing agreement between any UC Location and Supplier as of the Effective Date of this Agreement. For purposes of this Agreement, a UC Location shall include but not be limited to all current and future UC Locations of the University of California and its Affiliates as further detailed at <https://www.universityofcalifornia.edu/uc-system/parts-of-uc>.

1. Statement of Work

Supplier agrees to provide the Goods and/or described in the statement of work attached as **Attachment “A”** (“UC Statement of Work”) and any other documents referenced in the Incorporated Documents section herein, at the prices set forth in the UC Statement of Work and any other documents referenced in the Incorporated Documents section herein. Unless otherwise provided in the Agreement, UC will not be obligated to purchase a minimum amount of Goods and/or from Supplier.

2. Term of Agreement/Termination

- a. The Agreement is effective on the date of the final signature below (“Effective Date”). The initial term of the Agreement will be for 5 years after the Effective Date (Initial Term), and is subject to earlier termination as provided below.
- b. UC may renew the Agreement for up to five (5) successive 1-year periods (each, a “Renewal Term”), by providing Supplier with at least 30 calendar days’ written notice before the end of the Initial Term or any Renewal Term.
- c. UC may terminate the Agreement for convenience by giving Supplier at least 30 calendar days’ written notice.
- d. UC or Supplier may terminate the Agreement for cause by giving the other party at least 30 days’ notice to cure a breach of the Agreement (“Cure Period”). If the breaching party fails to cure the breach by the end of the Cure Period, the non-breaching party may immediately terminate the Agreement.

3. Scope of Agreement

- a) If Supplier eliminates any functionality of any of the Services provided under this Agreement and subsequently offers that functionality in other or new, similar products (whether directly or indirectly through agreement with a third party), then the portion of those other or new products that contain the functionality in question will be provided to UC at no additional charge and under the terms of this Agreement, including technical support. If Supplier incorporates the functionality of the Services provided under this Agreement into a newer product and continues to offer both products, UC may, in its sole discretion, exercise the option to upgrade to the newer product at no additional cost. Regardless of whether the functionality of the Services is impacted, Supplier will notify UC of any name changes in any Services within the earlier of thirty (30) calendar days of such change or thirty (30) days of when UC asks whether Supplier has made any name changes in the Services.
- b) UC and the users authorized by UC will have the right to access and use the Goods and/or Services at any location.

4. Rights and License In and To UC Data

- a) UC retains the right to use the Goods and/or Services to access and retrieve Non-public Information (as defined in the UC Appendix – Data Security and Privacy) stored on Supplier’s infrastructure at any time at UC’s sole discretion. If UC requests the Institutional Information from Supplier, Supplier will provide UC with copies within forty-eight (48) hours after receipt of a request from UC, and will cooperate with UC’s reasonable requests in connection with its response.
- b) UC will own all rights, title and interest in any and all intellectual property created in the performance of this Agreement by Supplier or its representatives to the extent expressly provided in a Statement of Work or other mutually agreed document as a “work made for hire” under U.S. copyright law, 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. In the event that it is determined that the “work made for hire” doctrine does not apply to such intellectual property, Supplier agrees to assign and hereby assigns to UC all rights, title, and interest in any and all intellectual property created in the performance of this Agreement, and will execute any future assignments or other documents needed for UC to document, register, or otherwise perfect such rights. UC acknowledges that Supplier may, from time to time during the term hereof for the benefit of its customers, update, enhance and/or modify its products and Goods and/or Services, and that such updates, enhancements and modifications shall constitute the exclusive property of Supplier.
- c) For the purposes of Article 8 of Appendix – Data Security and Privacy, Supplier will return all Institutional Information to UC in a commonly used, non-proprietary, and mutually agreed upon format.

5. Service Levels

- a) Supplier represents and warrants that the Goods and/or Services will be performed in a professional manner consistent with industry standards reasonably applicable to such Goods and/or Services.
- b) Supplier represents and warrants that the Goods and/or Services will be operational at least 99.99% of the time in any given month during the term of this Agreement, meaning that the outage or downtime percentage will be not more than .01%.
- c) If the Goods and/or Services’ availability falls below 99.99% in any month, Supplier will provide UC with a credit of that month’s bill for Goods and/or Services according to the table below.

AVAILABILITY PERCENTAGE	PERCENTAGE OF CREDIT
99.60% to 99.98%	10%
99.50% to 99.59%	20%
99.01% to 99.49%	30%
97.00% to 99.00%	50%
95.00% to 96.99%	75%
Below 95.00%	100%

- d) Supplier represents and warrants that ninety-five percent (95%) of all transactions will process within no more than one (1) second, and no single transaction will take longer than five (5) seconds to process.

- e) If UC has concerns regarding Supplier's service levels, UC may escalate these concerns to the following resource:

John Heuring – Director of Operations

Phone: 239-436-2753

Email: john.h@fischeridentity.com

- f) If Supplier's system response times fall below the warranted level for two (2) or more consecutive weeks, Supplier will provide UC with a credit in the amount of twenty percent (20%) of the Goods and/or Services fees for that month. If Supplier's system response times fall below the warranted level for six (6) out of eight (8) consecutive weeks, Supplier will be considered to be in default, and UC may, within sixty (60) days of such occurrence, terminate the Agreement without penalty.
- g) Supplier will provide UC with a refund for all unachieved service levels no later than the tenth (15th) business day of the month following the month in which the service levels was not achieved.
- h) Supplier will provide UC with monthly reports documenting its compliance with the service levels detailed herein. Reports will include, but not be limited to, providing the following information:
- i) Monthly Goods and/or Services availability by percent time, dates and minutes that Goods and/or Services were not available, and identification of months in which agreed upon service levels were not achieved;
 - ii) Average transaction processing time per week, the fastest and slowest individual transaction processing time per week, the percent of transactions processed that meet the service levels stated herein, and identification of weeks in which agreed upon service levels are not met.
- i) UC retains the right to retain a third party to validate Supplier's performance in meeting agreed upon service levels.

6. Technical Support

- a) During the term of this Agreement Supplier will provide UC with ongoing technical support for the Goods and/or Services at no less than the levels and in the manner(s) specified herein.
- b) Supplier may not withdraw technical support for any Service without twelve (12) months advance written notice to UC, and then only if Supplier is withdrawing technical support from all of its customers.
- c) UC acquires the right to access and use technical support acquired under this Agreement at any location.
- d) UC will receive at its option the general help desk technical support offered by Supplier to its other customers. Irrespective of Supplier's general technical support offerings, Supplier will provide UC at UC's option with the following technical support:
- i) Supplier will provide technical support to UC for the purpose of answering questions relating to the Goods and/or Services, including (a) clarification of functions and features of the Goods and/or Services; (b) clarification of the Documentation; (c) guidance in the operation of the Goods and/or Services; and (d) error

verification, analysis, and correction, including the failure to produce results in accordance with the Documentation.

- ii) Such assistance will be provided by Supplier twenty-four (24) hours a day, seven (7) days a week via a toll-free telephone number and live, online chat staffed by help desk technicians sufficiently trained and experienced to identify and resolve most support issues and who will respond to all UC requests for support within fifteen (15) minutes after receiving a request for assistance.
 - iii) Supplier will provide a current list of persons and telephone numbers for UC to contact to enable UC to escalate its support requests for issues that cannot be resolved by a help desk technician or for circumstances where a help desk technician does not respond within the time specified herein.
 - iv) Supplier provided telephone technical support will be compliant with Section 508 of the Rehabilitation Act.
- e) The following provisions will be applicable to the correction of Goods and/or Services errors:
- i) If UC detects what it considers to be an error in the Goods and/or Services which causes it not to conform to, or produce results in accordance with the Documentation, then UC will by telephone or e-mail notify Supplier of the error.
 - ii) Supplier will respond within two (2) hours to UC's initial request for assistance in correcting or creating a workaround for a Goods and/or Services error. Supplier's response will include assigning fully-qualified technicians to work with UC to diagnose and correct or create a workaround for the Goods and/or Services error and notifying UC's representative making the initial request for assistance of Supplier's efforts, plans for resolution of the error, and estimated time required to resolve the error.
 - iii) Within twenty-four (24) hours after UC first reports the error, Supplier will provide a correction or workaround acceptable to UC.
- f) The following provisions will set forth Supplier's obligations to provide enhancements to UC:
- i) Supplier will generally enhance and improve, update and correct the Goods and/or Services (each an "Enhancements") for as long as UC elects to receive and pays for the Goods and/or Services.
 - ii) Supplier will provide to UC during the Agreement term, (a) any and all Enhancements which it develops with respect to the Goods and/or Services; (b) any and all Enhancements required by federal or state governmental, or professional regulatory mandates related to UC's use of the Goods and/or Services; and (c) the Documentation associated with any Enhancements.
 - iii) Supplier will provide Enhancements to UC pursuant to subsection (ii) upon their general release and no later than the time when the first fifteen percent (15%) of Supplier's customers receive those Enhancements.
 - iv) Except as otherwise provided in a signed addendum to this Agreement, nothing herein will obligate Supplier to enhance the Goods and/or Services in any particular respect or on any particular date. The decision as to whether and/or when, to enhance the Goods and/or Services will be within Supplier's discretion.
- g) Supplier will provide UC with ninety (90) calendar days advance written notice of proposed product changes as well as product road maps relating to the Goods and/or Services provided to UC under this Agreement.

7. Purchase Order

- a. Unless otherwise provided in this Agreement, Supplier may not begin providing Goods and/or Services until UC approves a Purchase Order for the Goods and/or Services.
- b. Any purchase by any UC location of the Goods and/or Services included in this Agreement will be covered by the terms of this Agreement.

8. Invoices and Pricing

- a) Refer to Statement of Work or Purchase Order for Pricing. For systemwide agreements, each UC Location will specify the Invoicing Method and Payment Options that will apply, taking into account the operational capabilities of Supplier and the UC Location. See UC's Procure to Pay Standards [http://www.ucop.edu/procurement-Goods and/or Services/ files/Matrix%20for%20website.pdf](http://www.ucop.edu/procurement-Goods%20and/or%20Services/files/Matrix%20for%20website.pdf) for the options that will be considered. In the case of systemwide agreements, each UC Location will specify these terms in a Statement of Work or Purchase Order, as the case may be.]
- b. The Goods and/or Services will be available for UC purchase, at UC's sole discretion, during the term of this Agreement as stated herein.
- c. Supplier warrants that the pricing for the Goods and/or Services is no less favorable than the pricing it extends to Supplier's other government, non-profit and academic customers for the Goods and/or Services.
- d. All invoices must be itemized according to the Statement of Work and include the Agreement and/or Purchase Order Number, payment remittance instructions, and a description of the Goods and/or Services performed
- e. UC agrees to pay all net undisputed amounts due to Supplier in accordance with the Goods and/or Services fee schedule set forth below in Attachment B.
- f. If an invoiced amount is disputed in good faith by UC, then UC will work with the Supplier to resolve the dispute. UC may suspend the payment of all disputed amounts until the dispute is resolved. All of Supplier's obligations will continue unabated until dispute resolution.
- g. UC payment terms are net 30.
- h. Supplier will provide UC with quarterly monthly reports summarizing purchases made under this Agreement at no additional cost to UC.

9. Notices

As provided in the UC Terms and Conditions of Purchase, notices may be given by overnight delivery or by certified mail with return receipt requested, at the addresses specified below. Additionally, notices by Email will be considered legal notice if such communications include the following text in the Subject field: FORMAL LEGAL NOTICE – [insert, as the case may be, Supplier name or University of California].

To UC, regarding confirmed or suspected Breaches as defined under Appendix – Data Security and Privacy:

Name	Monte Ratzlaff		
Phone			
Email	Monte.Ratzlaff@ucop.edu		
Address	1111 Franklin Street, Oakland, CA 94607		

To UC, regarding Breaches or Security Incidents as defined under Appendix – Business Associate:

Name	Noelle Vidal		
Phone			
Email	Noelle.Vidal@ucop.edu		
Address	1111 Franklin Street, Oakland, CA 94607		

To UC, regarding contract issues not addressed above:

Name	Bala Balakumar		
Phone	310.794-6012		
Email	Bala.balakumar@ucop.edu		
Address	1111 Franklin Street, Oakland, CA 94607		

To Supplier:

Name	Ajith Domanic – Chief Information Security Officer		
Phone	239-436-2657		
Email	Ajith.d@fischeridentity.com		
Address	9045 Strada Stell Court Ste. 201 Naples, FL 34105		

10. Insurance

Supplier must deliver the Certificate of Insurance to UC's Buyer by email. Additionally, this requirement will be considered satisfied if a PDF version of the Certificate of Insurance is sent by Email and includes the following text in the Subject field: CERTIFICATE OF INSURANCE – Fischer Identity LLC

11. Intellectual Property, Copyright and Patents

The Goods and/or Services involve Work Made for Hire

The Goods/and Services and/or **do not** involve Work Made for Hire

12. Patient Protection and Affordable Care Act (PPACA)

Because they involve temporary or supplementary staffing, they are subject to the PPACA warranties in the T&Cs.

They do not involve temporary or supplementary staffing, and they are not subject to the PPACA warranties in the T&Cs.

13. Prevailing Wages

Supplier is not required to pay prevailing wages when providing the Goods and/or Services.

14. Fair Wage/Fair Work

Supplier is not required to pay the UC Fair Wage (defined as \$13 per hour as of 10/1/15, \$14 per hour as of 10/1/16, and \$15 per hour as of 10/1/17) when providing the Goods and/or Services.

15. Service-Specific Provisions

a. Additional Warranties:

- i. Goods and/or Services Warranty. Supplier represents and warrants that the Goods and/or Services provided to UC under this Agreement will conform to, be performed, function, and produce results substantially in accordance with the Documentation. Supplier will offer UC warranty coverage equal to or greater than that offered by Supplier to any of its customers.
- ii. Third Party Warranties and Indemnities. Supplier will assign to UC all third party warranties and indemnities that Supplier receives in connection with any Goods and/or Services provided to UC. To the extent that Supplier is not permitted to assign any warranties or indemnities through to UC, Supplier agrees to specifically identify and enforce those warranties and indemnities on behalf of UC to the extent Supplier is permitted to do so under the terms of the applicable Third Party agreements.
- iii. Date/Time Change Warranty. Supplier represents and warrants to UC that the Goods and/or Services provided will accurately process date and time-based calculations under circumstances of change including, but not limited to century changes, daylight saving time changes, leap year changes and leap second changes. Supplier must repair any date/time change defects at Supplier's sole expense.

16. Cooperative Purchasing

Supplier agrees to extend the terms of this Agreement to Participating Agencies (public and private schools, colleges and universities, cities, counties, non-profits, and all governmental entities) registered with OMNIA Partners, Public Sector. All contractual administration issues (e.g. terms and conditions, extensions, and renewals) will remain UC's responsibility except as outlined in the above referenced Request for Proposal "RFP 02197-SEPT2020 – UC Systemwide RFP for Information Technology Security Tools." Operational issues, fiduciary responsibility, payment issues, performance issues and liabilities, and disputes involving individual participating agencies will be addressed, administered, and resolved by each Participating Agency.

17. Incorporated Documents

The following documents are incorporated and made a part of this Agreement by reference as if fully set forth herein, listed in the order of precedence following the Agreement:

- a) Statement of Work – Attachment A
- b) **Redacted**
- c) UC Terms and Conditions of Purchase, dated 4/5/2021
- d) UC Appendix – Data Security and Privacy, dated 8/12/19
- e) UC Appendix – Business Associate, dated 8/2/2019

18. Entire Agreement

The Agreement and its Incorporated Documents contain the entire Agreement between the parties and supersede all prior written or oral agreements with respect to the subject matter herein. No click-through, or other end user terms and conditions or agreements (“Additional Terms”) provided with any Goods and/or Services or products hereunder will be binding on UC, even if use of such Goods and/or Services or products requires an affirmative “acceptance” of those Additional Terms before access is permitted. All such Additional Terms will be of no force and effect and will be deemed rejected by UC in their entirety.

The Agreement is signed below by the parties’ duly authorized representatives.

<p>THE REGENTS OF THE UNIVERSITY OF CALIFORNIA</p>	<p><small>DocuSigned by:</small> Justin Sullivan <small>C51AF9F2384C40B...</small></p>	<p><small>DocuSigned by:</small> <i>Daniel J. Dagnall</i> <small>4FE26C00BDF0465...</small></p>
---	---	---

<p>_____ (Signature) Justin Sullivan</p> <p>_____ (Printed Name, Title) 9/29/2021</p> <p>_____ (Date)</p>	<p>_____ (Signature) Daniel J. Dagnall</p> <p>_____ (Printed Name, Title) 9/28/2021</p> <p>_____ (Date)</p>
---	---

Attachment A to Purchasing Agreement # 2021003140

UC Statement of Work

1. Description of the Scope of Services:

The purpose of this Statement of Work is for Supplier to provide the University with Identity Governance and Admin tools (including as applicable Professional Services) and related tools and Goods and/or Services, in a cost effective and efficient manner, accompanied by high standards of quality and service, aligned with University's needs as further detailed herein.

Prior to any engagement between the University and the Supplier, a UC location specific Statement of Work referencing the terms of this Agreement shall be negotiated between the UC location (s) and Supplier outlining all key tasks and work activities including but not limited to discovery, migration, solution construction, implementation plan, all deliverables, completion timeline, project management schedule, performance-based milestone payment schedule for professional services during implementation, key personnel, reporting requirements, escalation path, assumptions, obligations of each party, how changes to the Services are managed and end user acceptance criteria and testing.

The effective date of the term of any Goods and/or Services acquired under this Agreement shall be the date the UC Location has approved that the Goods and/or Services are fully functional in a production environment.

Supplier must provide the necessary staff, infrastructure, and other resources at a level sufficient to ensure efficient, effective, and continually improving fulfillment of its obligations under this Agreement. Supplier's provision of the Goods and/or Services must always be in a manner and level equal to or greater than as detailed in Supplier's Response to the UC RFP 002197-SEP2020 – UC Systemwide RFP – Information Technology Security Tools ("RFP") which is attached as Exhibit 1 the Statement of Work.

2. Participating Locations

Supplier shall make all terms of the Agreement available to all current and future locations of the University of California and its Affiliates as further detailed at <https://www.universityofcalifornia.edu/uc-system/parts-of-uc>.

3. Sustainability:

Supplier will register and participate in an assessment of their sustainability practices and procedures through the EcoVadis Corporate Social Responsibility (CSR) monitoring platform. For more information on the EcoVadis platform and costs associated with an assessment, please see the EcoVadis Supplier Solutions Website here: <https://www.ecovadis.com/us/supplier-solutions-2/>.

4. Pricing:

During the Initial Term and any subsequent Renewal Terms, the prices of Supplier's Goods and Services as reflected as Attachment B to the Purchasing Agreement shall not increase.

Exhibit 1 to Statement of Work

Fischer response to the UC RFP 002197-SEP2020 – UC Systemwide RFP – Information Technology Security Tools (Identity Management Solutions category)

Table 1 Supplier Capability

1	Are you a manufacturer (OEM), Value Added Reseller (VAR), or distributor.	Manufacturer
2	Is the OEM going to submit the response to this RFP directly and be responsible for fulltime and distribution of the product(s)?	Yes
3	If the OEM is going to submit the response to this RFP with coordination and collaboration with a channel partner for fulfillment and distribution of the product(s), the UC requires a Master Agreement with the OEM in addition to a purchasing agreement with the channel partner. Please acknowledge your acceptance of this requirement.	N/A
4	If a VAR/Channel partner is going to submit the response to this RFP with coordination and collaboration with an OEM with the channel partner for fulfillment and distribution of the product(s) attach a letter of attestation signed by the OEM stating the nature of the collaboration	N/A
5	Please describe your company's capability of providing full service to all UC Locations. Describe your distribution model, including the size and location of your company's distribution facilities, warehouses and retail network.	Fischer Identity software is distributed electronically via our support portal. We currently support the following California campuses: Pepperdine, CSU East Bay, CSU Bakersfield, CSU Chico and CSU San Bernardino.
6	Will your company's employees who are responsible for providing Services to your customers conform to the following? If so, please describe: Carry Picture ID, have passed background security checks?	Yes, Fischer Identity employees will carry a picture ID and. An extensive background check is part of our employee hiring process.

7	<p>Describe the account management team, and all roles thereunder, that you would assign to the UC system if awarded under this RFP, including senior account manager responsible for the entire agreement and UC relationship and local account representatives responsible for each specific UC location. Include attachment if necessary</p>	<p>Fischer Identity Account Management Team</p> <p>Fischer has the staff and resources to meet UC System project goals and timelines. Fischer has been providing Identity Management services since 2005. Today, Fischer has arguably become the most experienced and knowledgeable identity management vendor in the industry. Fischer Specializes in Higher Education, Over 100 campuses use Fischer Identity products and services. Given our history and experience, we are in a unique position to provide best practices recommendations at multiple levels. Fischer offers an implementation methodology that focuses on and exposes these best practices and we have found it to be the roadmap to a successful deployment. Our customers are testimony to this fact. Fischer has developed a phased project implementation methodology that ensures customer solutions are built on-time, within budget, and to the customer's business and technical requirements. This proven methodology allows Fischer to consistently deliver quality and predictable IdM implementations and in timeframes that are drastically shorter than conventional IdM projects. Fischer solutions are typically delivered in 8 to 12 weeks post execution of the Statement of Work.</p> <p>Fischer's project methodology and project plan is designed to proactively mitigate risk of impediments during the implementation. Fischer's project approach is Fixed Fee/Milestone based with client acceptance required. We are confident in our solution and implementation services and this approach turns any risk to Fischer.</p> <p>Fischer reserves the right to assign or not assign a project manager based on the overall dynamic of the project team.</p> <p>Fischer does not actively staff a project management group, rather we assign principal architects that stay attached</p>
---	---	--

		throughout the solution. The timing of your project, will determine which architect and project staff are assigned .
8	If you are a VAR or distributor, what is the average response time for an account manager(s) to respond to initial requests?	N/A
9	Identify any partners, subcontractors or any other staff/personnel resources outside of your company that you are partnering to perform the Goods and/or Services contemplated under this RFP and the role they play in performing the Goods and/or Services.	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. The decision to initiate a 3rd party integrator relationship is largely tied to the availability of people to staff the deployment correlated with the customer's timeline / deadline needs and goals. We are fully transparent in this process and always discuss the available options with the customer

		<p>before making a final decision to engage a partner or not.</p>
10	<p>Please specify your company's normal business hours in Pacific Time zone format for receiving orders and providing customer service including maintenance support both during and after normal business hours.</p>	<p>Fischer's Naples, FL office is open from 8:00 AM - 5:00 PM EST. Out West Coast Sales Director is available from 8:00 AM - 5:00 PM PST. Support is available 24/7 365 days a year. Customers may request support via telephone, Fischer's Online Customer Support Portal, email or fax. Fischer utilizes various technologies to facilitate remote problem determination. The process allows Fischer to remotely identify and troubleshoot issues regarding the Identity Product Suite. Fischer Technical Support is dedicated to resolving Priority 1 problems as quickly as possible by working around the clock with the customer until the problem is resolved.</p>

11	Describe your quoting process and how you will meet our requirement of providing assistance with product sales questions, technical inquiries and customer service inquiries	<p>We use a fixed cost, milestone-based services model with client acceptance required instead of a Time and Materials T&M approach. To ensure accuracy we perform more intensive discovery and solution design, which enables us to provide an accurate fixed cost services quote based on the project phase requirements. All quotes and milestones, include time for project management and solution construction, which explains the variable FTE counts on our end. If a single FTE number is indicated, please note that it still includes some time for project management. We are confident in our solution and implementation services and this approach turns any risk to Fischer. If UC System would like Time and Material rates for the hour increments indicated we will work with you to provide an hourly rate. Support is included with the Annual Software Maintenance Fee or Annual IaaS[®] Subscription Fee, as applicable. Support is available 24/7 365 days a year. Customers may request support via telephone, Fischer's Online Customer Support Portal, email or fax. Fischer utilizes various technologies to facilitate remote problem determination. The process allows Fischer to remotely identify and troubleshoot issues regarding the Identity Product Suite. Fischer Technical Support is dedicated to resolving Priority 1 problems as quickly as possible by working around the clock with the customer until the problem is resolved.</p>
----	--	--

<p>12</p>	<p>Explain how your company proposes to resolve any complaints, issues, or challenges. Please detail your company's problem resolution and escalation process for customer complaints and concerns.</p>	<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.</p> <p>The levels of service provided by Fischer to Licensee are described below.</p> <p>Priority 1 Support Requests: Fischer technical support personnel work around the clock until the problem is resolved. It is critical that an Authorized Licensee 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.</p> <p>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 Licensee 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.</p> <p>Priority 3 and Priority 4 Support Requests: Fischer will schedule work as appropriate. Resolution may be provided in the next scheduled product release.</p> <p>Support Requests are automatically escalated to higher levels within Fischer as provided in the table below.</p> <p>Fischer Escalation for Support Requests</p> <p>Priority</p> <p>Criteria for Escalation Within Fischer</p> <p>Notification to</p>
-----------	---	---

		<p>Priority 1 Critical</p> <p>Every 2 hours from time of creation or last update</p> <ol style="list-style-type: none">1. Director of Operations2. Support Manager3. Primary Support Specialist <p>Priority 2 High</p> <p>Every 4 hours from time of creation or last update</p> <ol style="list-style-type: none">1. Support Manager2. Primary Support Specialist <p>Priority 3 Medium</p> <p>No Response to Licensee which may include plans for a Workaround or a Fix in the next release has been communicated to Licensee within in 1 business day.</p> <ol style="list-style-type: none">1. Support Manager2. Primary Support Specialist <p>Priority 4 Low</p> <p>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.</p> <ol style="list-style-type: none">1. Support Manager2. Primary Support Specialist
--	--	---

13	<p>Describe your ability to regularly provide electronic reports (in Microsoft Excel and other formats) providing a wide range of information related to the resulting agreement at both the UC-wide level and for each individual UC location including, but not limited to quarterly usage reports. Data provided in the reports should include, but not be limited to: UC Location, UC Department, UC Purchase Order Number, Name and Model of Service(s) purchased, usage volumes, discount percent, MSRP, UC final discounted price, price paid, per unit and total</p>	<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. Authorized users e.g. Administrators and Auditors can login into self-service to configure, run view and share the reports.</p>
14	<p>Describe what else your company will do to support UC's overall mission during the term of the agreement? UC's mission statement is available at: https://www.ucop.edu/uc-mission/.</p>	<p>Our Mission...Your Success!</p>

Table 2 Supplier Support

1	<p>Describe all maintenance and support packages, and summarize the services, deliverables and terms included (for example, bug fixes, patches, service packs and associated services).</p>	<p>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 % of the license charge. See attached Maintenance and Support document and Master Subscription Agreement document.</p> <p>Software Upgrades</p> <p>Fischer releases in the Agile model with continuous integration. Documentation is included in each build and can be downloaded from our FTP site.</p> <p>Our goal is 1 major release per year with 2 - 3 minor release and patches as necessary. We currently support 3 major releases.</p> <p>Our versioning model consists of three numbers as: MAJOR.MINOR.PARTCH.</p> <p>MAJOR: it will be incremented based on a business decision, if the release is considered large, it will be incremented. MINOR: when new features are added to the product, the minor will be incremented. PATCH: any bug requiring a fix will trigger incrementing this value.</p> <p>For our hosted IaaS customers upgrades are required and performed by Fischer once per quarter, as needed. The maintenance window to perform Service Pack upgrades is typically 1 - 2 hours and they are applied during off-peak times during the early morning hours. During this time, Provisioning processes are suspended and users are presented with a prompt to indicate that the solution is currently undergoing maintenance when attempting to login to self-service to perform</p>
---	---	--

		<p>password resets, profile updates, etc. Hotfixes do not require a maintenance window or outage period. As with any upgrade, Fischer thoroughly tests all updates, prior to applying the update to client production environments.</p> <p>For our on-premises customers, upgrades and patches are available for download via our secure SFTP site. Availability of updates are communicated via an e-mail distribution list to our customers.</p> <p>Prior to releasing any Service Pack, Fischer will send an e-mail notification to the client at least 30 days in advance of the scheduled upgrade. The notification specifies the date and time of when the upgrade will be deployed and the expected outage duration. If the client has a Test environment, the Service Pack will be deployed two weeks prior to upgrading the Production environment. This allows for adequate time for the client to test functionality, if they choose to do so.</p> <p>Security Patches and Bug Fixes</p> <p>Fischer Identity's SaaS platform is configured to harden security to very high standards. Periodic and ad hoc application of security patches when vendors release them is in place. All components and operating platform used in the SaaS environment are patched to the latest security update. Fischer also performs periodic security assessments for the application and fixes all potential issues. Fischer will perform due diligence immediately to determine the impact of the bug or issue. Once a course of action is decided we work with our customers to ensure they are notified of the issues that affect our platform as well as the specific mitigation methods we plan to employ. This includes any recommendations to our customers related to actions they should take as a result of a newly exposed bug or issue with security and the underlying components.</p> <p>See Attachment A Maintenance and Support.docx</p>
--	--	---

2	How is the customer notified for vulnerabilities or patch updates?	<p>Prior to releasing any Service Pack, Fischer will send an e-mail notification to the client at least 30 days in advance of the scheduled upgrade. The notification specifies the date and time of when the upgrade will be deployed and the expected outage duration. If the client has a Test environment, the Service Pack will be deployed two weeks prior to upgrading the Production environment. This allows for adequate time for the client to test functionality, if they choose to do so.</p> <p>Security Patches and Bug Fixes</p> <p>Fischer Identity's SaaS platform is configured to harden security to very high standards. Periodic and ad hoc application of security patches when vendors release them is in place. All components and operating platform used in the SaaS environment are patched to the latest security update. Fischer also performs periodic security assessments for the application and fixes all potential issues. Fischer will perform due diligence immediately to determine the impact of the bug or issue. Once a course of action is decided we work with our customers to ensure they are notified of the issues that affect our platform as well as the specific mitigation methods we plan to employ. This includes any recommendations to our customers related to actions they should take as a result of a newly exposed bug or issue with security and the underlying components.</p>
---	--	---

3	Do you have a development team that is responsive to new feature requests ?	<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.</p> <p>Currently our online support portal serves as our central location for product enhancement request and product updates. Customers can use the Self-Service support portal to submit enhancement requests and track the requests as they progress through the Software Development Life Cycle. The queue of enhancements requests is reviewed monthly in our strategic planning meetings by product owners, developers and the implementation team. Enhancements requests are vetted and added to product planning and product roadmap where applicable.</p>
---	---	--

<p>4</p>	<p>Describe your upgrade process (include communication points and lead-time notification). Identify if it is a re-implementation.</p>	<p>Upgrades are completed at no cost.</p> <p>Fischer releases in the Agile model with continuous integration. Documentation is included in each build and can be downloaded from our FTP site.</p> <p>Our goal is 1 major release per year with 2 - 3 minor release and patches as necessary. We currently support 3 major release levels.</p> <p>Our versioning model consists of three numbers as: MAJOR.MINOR.PARTCH.</p> <p>MAJOR: it will be incremented based on a business decision, if the release is considered large, it will be incremented. MINOR: when new features are added to the product, the minor will be incremented. PATCH: any bug requiring a fix will trigger incrementing this value.</p> <p>For our hosted IaaS customers upgrades are required and performed by Fischer once per quarter, as needed. The maintenance window to perform Service Pack upgrades is typically 1 - 2 hours and they are applied during off-peak times during the early morning hours. During this time, Provisioning processes are suspended and users are presented with a prompt to indicate that the solution is currently undergoing maintenance when attempting to login to self-service to perform password resets, profile updates, etc. Hotfixes do not require a maintenance window or outage period. As with any upgrade, Fischer thoroughly tests all updates, prior to applying the update to client production environments.</p> <p>For our on-premises customers, upgrades and patches are available for download via our secure SFTP site. Availability of updates are communicated via an e-mail distribution list to our customers.</p> <p>For our hosted IaaS customers upgrades are required and performed by Fischer once per quarter, as needed. The maintenance window to perform Service Pack upgrades is typically 1 - 2</p>
----------	--	--

		<p>hours and they are applied during off-peak times during the early morning hours. During this time, Provisioning processes are suspended and users are presented with a prompt to indicate that the solution is currently undergoing maintenance when attempting to login to self-service to perform password resets, profile updates, etc. Hotfixes do not require a maintenance window or outage period. As with any upgrade, Fischer thoroughly tests all updates, prior to applying the update to client production environments.</p> <p>For our on-premises customers, upgrades and patches are available for download via our secure SFTP site. Availability of updates are communicated via an e-mail distribution list to our customers.</p>
--	--	--

5	Can upgrades be deferred and schedule as needed?	<p>For our hosted IaaS customers upgrades are required and performed by Fischer once per quarter, as needed. The maintenance window to perform Service Pack upgrades is typically 1 - 2 hours and they are applied during off-peak times during the early morning hours. During this time, Provisioning processes are suspended and users are presented with a prompt to indicate that the solution is currently undergoing maintenance when attempting to login to self-service to perform password resets, profile updates, etc. Hotfixes do not require a maintenance window or outage period. As with any upgrade, Fischer thoroughly tests all updates, prior to applying the update to client production environments.</p> <p>For our on-premises customers, upgrades and patches are available for download via our secure SFTP site. Availability of updates are communicated via an e-mail distribution list to our customers.</p>
6	Is there a Technical Account Manager assigned to the portfolio for escalations?	<p>Yes, 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>
7	Describe geographical location and structure of your support team.	<p>Our Solution Management team is responsible for handling support requests, as well as solution change requests. The team consists of 10 technical staff members, 7 of which are based out of our Naples, FL headquarters and 3 that are based out of our Trivandrum, India office.</p>
8	Is support available via telephone, email, remote access.	<p>Support is included with the Annual Software Maintenance Fee or Annual IaaS® Subscription Fee, as applicable. Support is available 24/7 365 days a year. Customers may request support via telephone, Fischer's Online Customer Support Portal, email or fax. Fischer utilizes various technologies to facilitate remote problem determination. The process allows Fischer to remotely identify and troubleshoot issues regarding the Identity Product Suite. Fischer Technical Support is dedicated to resolving Priority 1 problems as quickly as possible by working around the clock with the customer until the problem is resolved.</p>

<p>9</p>	<p>Describe support plan options, including general service level commitments offered under this support agreements.</p>	<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>The levels of service provided by Fischer to Licensee are described below.</p> <p>Priority 1 Support Requests: Fischer technical support personnel work around the clock until the problem is resolved. It is critical that an Authorized Licensee 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.</p> <p>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 Licensee 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.</p> <p>Priority 3 and Priority 4 Support Requests: Fischer will schedule work as appropriate. Resolution may be provided in the next scheduled product release.</p> <p>Support Requests are automatically escalated to higher levels within Fischer as provided in the table below.</p> <p>Fischer Escalation for Support Requests</p> <p>Priority</p> <p>Criteria for Escalation Within Fischer</p>
----------	--	--

		<p>Notification to</p> <p>Priority 1 Critical</p> <p>Every 2 hours from time of creation or last update</p> <ol style="list-style-type: none">1. Director of Operations2. Support Manager3. Primary Support Specialist <p>Priority 2 High</p> <p>Every 4 hours from time of creation or last update</p> <ol style="list-style-type: none">1. Support Manager2. Primary Support Specialist <p>Priority 3 Medium</p> <p>No Response to Licensee which may include plans for a Workaround or a Fix in the next release has been communicated to Licensee within in 1 business day.</p> <ol style="list-style-type: none">1. Support Manager2. Primary Support Specialist <p>Priority 4 Low</p> <p>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.</p> <ol style="list-style-type: none">1. Support Manager2. Primary Support Specialist
--	--	--

10	Is support available via telephone, email, remote access.	Support is included with the Annual Software Maintenance Fee or Annual IaaS® Subscription Fee, as applicable. Support is available 24/7 365 days a year. Customers may request support via telephone, Fischer's Online Customer Support Portal, email or fax. Fischer utilizes various technologies to facilitate remote problem determination. The process allows Fischer to remotely identify and troubleshoot issues regarding the Identity Product Suite. Fischer Technical Support is dedicated to resolving Priority 1 problems as quickly as possible by working around the clock with the customer until the problem is resolved.
11	Describe the use of internet-based support of the solution including knowledgebase and technician access (online chat).	Fischer has a searchable knowledge base "FRED" Fischer Repository for Essential Data that includes our entire product guide, as well as frequently asked questions. Fischer provides a web-based support portal for customers to report incidents, solution change requests, and inquiries. Fischer maintains the name, date, time, and priority of the deficiency/enhancement as well as the nature of the deficiency/enhancement, current status, action plans, dates, and times, expected and actual completion time, and resolution information. Customer have access in the support portal to chat with support personnel, view, comment and escalate if necessary.

<p>12</p>	<p>Describe service level response times during regular support hours as well as levels of support outside of regular support hours. The response should include by Severity Level the number of hours within which a response can be expected for non-emergency and emergency (production-down) inquiries. In addition, the response should define the duration within which a resolution is expected - for both non-emergency and emergency (production down) inquiries.</p>	<p>The levels of service provided by Fischer to Licensee are described below.</p> <p>Priority 1 Support Requests: Fischer technical support personnel work around the clock until the problem is resolved. It is critical that an Authorized Licensee 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.</p> <p>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 Licensee 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.</p> <p>Priority 3 and Priority 4 Support Requests: Fischer will schedule work as appropriate. Resolution may be provided in the next scheduled product release.</p> <p>Support Requests are automatically escalated to higher levels within Fischer as provided in the table below.</p> <p>Fischer Escalation for Support Requests</p> <p>Priority</p> <p>Criteria for Escalation Within Fischer</p> <p>Notification to</p> <p>Priority 1 Critical</p> <p>Every 2 hours from time of creation or last update</p> <ol style="list-style-type: none"> 1. Director of Operations 2. Support Manager 3. Primary Support Specialist
-----------	--	--

		<p>Priority 2 High</p> <p>Every 4 hours from time of creation or last update</p> <ol style="list-style-type: none">1. Support Manager2. Primary Support Specialist <p>Priority 3 Medium</p> <p>No Response to Licensee which may include plans for a Workaround or a Fix in the next release has been communicated to Licensee within in 1 business day.</p> <ol style="list-style-type: none">1. Support Manager2. Primary Support Specialist <p>Priority 4 Low</p> <p>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.</p> <ol style="list-style-type: none">1. Support Manager2. Primary Support Specialist <p>Attachment B: Fischer - IaaS Cloud SLAs.pdf</p>
--	--	---

<p>13</p>	<p>Do you offer stand-up meetings to go over progress, questions, feedback etc.?</p>	<p>Implementation and Execution:</p> <p>Fischer's project methodology and project plan is designed to proactively mitigate risk of impediments during the implementation.</p> <p>Quality Assurance Checkpoints</p> <p>We use daily standup meetings as well as quality assurance checkpoints to make sure the work we are performing is on task and meets your project goals and requirements. If a scope change is identified, we will perform discovery on the new requirement, determine the level of effort and issue a project change request to be approved by the customer prior to commencing any work for the proposed change.</p> <p>Fischer Identity will provide weekly progress/status reports.</p> <p>At the end of each sprint, the Implementation team performs internal end-to-end and unit testing to ensure that the logic in place is functioning per the customer requirements. During the Quality Assurance checkpoints, Fischer also provides the customer with a solution showcase that entails the Fischer Implementation team member demonstrating the logic of the workflows that were built, as well as demonstrating the functionality of the customer use cases that were built during the associated sprint. The Quality Assurance checkpoints are not only designed to ensure that the solution has been tested per our QA standards, but also to ensure that the solution is being constructed per your requirements.</p> <p>Scope Management</p> <p>During the implementation, if an additional requirement is identified that falls outside of the agreed upon solution design and statement of work, i.e. "scope creep", Fischer will work directly with the customer to determine the scope of the change and level of effort involved in accommodating the change. Once scoped, Fischer will issue a Project Change Request PCR that will require sign-off by the customer project sponsor and Fischer Management.</p>
-----------	--	--

14	Do you have a training catalog and curriculum available for selection at the customer's discretion	<p>Fischer Identity provides onsite training 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.</p> <p>All customer training and the associated material is created based on the specific design and functionality of the customer's solution. We utilize members of our Implementation and Solution Management teams to perform the training. Each team member has extensive knowledge of the Fischer product and have all facilitated training sessions with our customers. Fischer Product guides and solution documentation are provided as part of the training.</p> <p>Topic covered in basic training include: Managing Approvals; Adding Policies and Roles, Configuring Password management. Topic covered in advanced training include: Applying Patches and Managing Workflow Processes.</p> <p>For end users, Fischer offers "train the trainer" courses based on the modules being utilized. This approach allows your staff to train the user population as needed and typically reviews all end user interfaces your users will encounter.</p> <p>Fischer also offer the Fischer Identity Guru Training Program for customer who would like to purchase additional training.</p> <p>Fischer Identity offers both basic and advanced training. For customers administering their own solution, Fischer offers week-long Basic and Advanced Fischer Identity training courses for administrators. This can be held onsite, remotely through web-conference or at the Fischer Corporate Headquarters in Naples, FL. The training agenda is created for your solution, covering all areas your staff will need to understand how the product is integrated and deployed. Topic covered in basic training include: Managing Approvals, Adding</p>
----	--	--

		<p>policies roles, and Configuring Password management. Topic covered in advanced training include: Applying Patches and managing workflow processes. This training can be done either at your location or at the Fischer corporate headquarters in Naples Florida. T&E will apply.</p> <p>For customers with Identity as a Servicer cloud subscriptions, Fischer offers "train the trainer" courses based on the modules being utilized. This approach allows your staff to train the user population as needed and typically reviews all end user interfaces your users will encounter. This training is typically delivered remotely due to its short duration; however, training can be done at your location if preferred. T&E will apply.</p> <p>There are no industry certifications directly related to Identity Access Management.</p> <p>Fischer Identity offers a comprehensive training & certification platform called the Identity GURU program. This program focuses not only on training but certifying resources to ensure that they have an understanding of the typical Identity and Access Management IAM challenges facing organization today but also offers a complete 360 degree view of the Fischer Identity platform and its flexible deployment model. All training is available via our cost effective yearly subscription model. This model allows customers to tailor their training needs to meet their desired business objectives.</p> <p>We offer the following training experiences:</p> <p>Fischer University - Online courses and learning tracks that are focused on understanding Identity and Access Management, and understanding the capabilities, solution implementation and management of the Fischer Identity platform.</p> <p>Paradise Program - Classroom based training located at our Naples based headquarters. Sessions are scheduled to minimize the impact to the day to day job responsibilities of the attendees. These sessions are a focused, in-depth review of the content available on the Fischer University.</p>
--	--	---

		<p>Customer Specific - Training agendas are tailored to meet a customer's specific objectives and are held onsite at a location of their choosing.</p> <p>Best Practices - Business Analysis workshop that help customers focus on high-level solution requirements and the development of an IAM roadmap for the implementation of their IAM requirements and business objectives.</p> <p>Customers can consume the above training in one of the following subscription levels, these levels allow customers to choose the types of training required for their users:</p> <p>Basic - All available online Fischer University content.</p> <p>Intermediate - Basic Level + Paradise Program</p> <p>Advanced - Intermediate Level + Customer Specific</p> <p>Platinum - Advanced Level + Best Practices</p> <p>Once subscribed, customers are allocated an appropriate number of seats based on the level chosen. If additional seats are required, they can be allocated for an additional charge.</p> <p>Attachment C : Training</p>
--	--	---

Table 3 Identity Governance (Part A)

1	Does your solution offer all capabilities asked in this questionnaire within a single product or does it require purchase of multiple products? If multiple, list all products	Fischer offers all capabilities asked in this questionnaire in a single product.
2	Provide name and version of all the product(s) whose features and functionality is included in the responses below.	Fischer Identity Version 7.5.7
3	Describe the vision and direction for the products in this category	<p>Fischer has been delivering cloud-based IdM for more than nine 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 UC System user population, Fischer is concentrating its development efforts to extend or add these capabilities.2021:</p> <ul style="list-style-type: none"> • The ability for customers / partners to build their own end point integrations to Fischer • A new Access Management Solution supporting, SAML, CAS, OIDC, OAuth and ADFS protocols including user managed access and PEP/PDP enforcement • 100% REST API code coverage • Updated AngularJS end user interface (fully

		<p>responsive)</p> <ul style="list-style-type: none">• Identity Analytics• Upgrades to Compliance to provide more real-time governance• Cybersecurity and fraud detection / mitigation solutions <p>2022:</p> <ul style="list-style-type: none">• Native Windows integration at the PC level for Identity related actions (i.e. upgraded credential provider)• A new, extensive Identity Schema to meet integration and other Identity-related demands and use cases• Updated Administration experience as an augmentation to our new AngularJS interface• Rapid deployment upgrades to our already best of breed deployment model. <p>2023:</p> <ul style="list-style-type: none">• Containerization of the product from an “official delivery / installation” perspective (Fischer can already be docker-ized today)• Expansion of our service-delivery model• Embedded Role Mining & Role Discovery Services expanding on our current approach. <p>2024:</p> <ul style="list-style-type: none">• Machine Learning and AI type services (most likely delivered before 2024) <p>2025:</p> <ul style="list-style-type: none">• De-centralized / Distributed Identity upgrades to provide more CIAM-type services and features than we have available today. <p>Note: This roadmap is subject to change and some enhancements may be delivered soon or later depending upon factors beyond our control.</p>
--	--	---

4	List your top 5 technology alliances with information technology vendors in this category	<p>https://www.fischeridentity.com/partners/</p> <p>1Kosmos - Identity Proofing</p> <p>Vendor Unamed for confidentiality - Fraud / Breach Protection</p> <p>TransUnion - MFA / Adaptive Access Control</p> <p>Vendor Unamed for confidentiality - Identity Analytics</p> <p>Ellucian Partner - Ellucian is the technology leader of software and services powering higher education forward.</p> <p>Ellucian Ethos Connected Partner - Ethos is the higher education framework connecting people, processes and applications across the institution to power coordinated programs designed for student success.</p>
---	---	---

<p>5</p>	<p>Describe your product differentiators versus other competitive products in this category</p>	<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> <p>Fischer's Workflow and Connectivity Studio – Our Workflow and Connectivity Studios is where we truly differentiate ourselves from the competition. We have abstracted the coding layer a zero-coding approach to building workflows. You do not need to be an expert in any programming or scripting language, rather we have normalized the skillset required to build enterprise grade identity management workflows. Our studio provides visual tools, intuitive design and data mapping functionality, connectivity and schema discovery in a visual drag and drop WYSIWYG usability to build complex workflows without the traditional coding or scripting required in other identity systems. To accompany this Fischer provides templates and schemas that we have developed and deployed over time in other institutions to expedite delivery. .</p> <p>Higher Education specialization -</p> <p>Fischer is the number one provider of Identity Management Services for Higher Education. Over 100 campuses use Fischer Identity products and services, with many more planning to leverage their same success.</p> <p>We understand higher education processes, systems/technical environments, users, business challenges, goals, and missions.</p>
----------	---	--

		<p>Choice of Deployment Model: on-campus software or hosted cloud subscription.</p> <p>Ease and Speed to change and extend the solution to meet new business requirements.</p> <p>Higher Education Experience: Fischer has over 10 years of experience in cloud based Identity Access Management.</p> <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>
--	--	--

6	List all license models (On Prem, SaaS, Perpetual, Term) offered for the product(s) you are quoting in this category	Fischer supports on-premises, IaaS hosted managed by Fischer. SaaS managed by UC System and hybrid software delivery models. The Product features are the same for all solutions. 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. We have moved a customer from our cloud data centers to on premises in a weekend. It is a very straight forward process. The system is purpose built to be streamlined in deployment, delivery, implementation and ongoing value. The architecture is built to provide efficiency in operation while providing for powerful configuration options to meet the needs of even the most complex identity management requirements in higher education. The foundation is an integrated solution with deep bi-directional connectivity, powerful configuration options that allows for customized identity solutions without coding. With the constant involvement of our customers, astute market awareness in cyber security and the resources to maintain the future of the solution, the flexible architecture allows Fischer to keep up with the needs of identity management. Going into the future with continuing evolution as demonstrated by our first to market Identity as a Service and visual design studio, supported by our Global Gateway architecture. Now available in flexible deployment as true, full featured SaaS without compromise of functionality allowing delivery of the full power of the solution for any identity, and protocol, anywhere.
7	List and describe any related products and services not included in this Request for Proposal that your firm can provide that may be of benefit to the University. (See IT Security Price file in Pricing Questionnaire for instructions on providing pricing)	Fischer provides all professional implementations services for our clients, including pre-sales discovery, solution discovery, solution architecture and design, workflow development, infrastructure support, installation, and training. Organizations may elect to have any one of Fischer's qualified implementations partners provide some or all of the associated professional services. Fischer also provides, directly and through solution partners, consulting and assessment services related to IGA strategy, assessment, and process.

8	<p>Describe your professional services offerings including but not limited to the following the approach for deploying the service and integrating with location business processes which defer from campus to campus</p>	<p>Once the Fischer Implementation team has completed the Solution Construction phase, the solution is turned over to the customer to perform user acceptance testing. All interfaces are tested during UAT and prior to Go-Live. All customizations are tested.</p> <p>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.</p> <p>Completion of UAT and customer acceptance of UAT signify that the as built solution meets the customer requirement and is ready to be migrated to production. In preparation for go live during the production migration phase we test to ensure successful connectivity to all target systems and applications.</p>
9	<p>Describe your professional services offerings including but not limited to discovery/import of privileged accounts and target systems Administrative authentication configuration (MFA required).</p>	<p>Fischer is setting unprecedented deployment times as a result of "configuration vs. customization" approach, Agile project methodology, and strong project management.</p> <p>Statement of Work - As part of the implementation proposal, Fischer Identity will include the UC Riverside project team to jointly develop a detailed SOW. Fischer conducts a one week workshop that can be held onsite or remotely. The purpose of the workshop is to work directly with your staff to gather all the requirements. Once the requirements are agreed upon, the statement of work is created.</p> <p>Scope of Work - An extensive review of the statement of work is conducted until both parties agree to the scope of work. The statement of work is the foundation which the implementation team will begin the implementation work for the project.</p>

<p>10</p>	<p>Describe your professional services offerings including but not limited to the following: Installations and configuration; architecture/strategy/planning</p>	<p>Fischer to consistently deliver quality and predictable IdM implementations and in timeframes that are drastically shorter than conventional IdM projects.</p> <p>Fischer solutions are typically delivered in 8 to 12 weeks post execution of the Statement of Work. See Attachment E - Fischer Implementation Methodology.</p> <p>Hardware, Network, and Software configuration and installation is encompassed in Phase III, IV, and V in the attached Fischer Implementation Methodology. In order to perform work during these phases, Fischer strongly recommends that the client provide Fischer personnel with VPN access to their network.</p> <p>Phase III - Platform Installation and Configuration During this phase, Fischer works directly with the appropriate client IT personnel to begin the build out of the infrastructure that is required to support the Fischer product and solution. Essential client personnel that are required during this phase are those who are responsible for Operating System installations, configuring web servers, and installing any 3rd party components that may be necessary. IT personnel typically include Network Administrators, MIS professionals, application analysts, etc.</p> <p>Phase IV - Network Configuration Network configuration that is required to support the Fischer product are the responsibility of the client. Requirements are provided to the client by Fischer. Network configuration includes, but are not limited to, configuration of client firewalls, SSL, and load balancer if applicable.</p> <p>Phase V - Application Tier Install/Configuration During Phase V, Fischer personnel perform the installation of the Fischer product.</p> <p>For on premise, we recommend 2 provisioning and web servers to ensure high availability. See Attachment F - Official Cloud Pre Requisites Guide.</p>
-----------	--	---

		<p>For IaaS Managed Services we require 2 GIGs installed within your network to facilitate communication between our cloud and your on-premise environment. See Attachment G - Official On-Prem Pre Requisites Guide.</p>
--	--	---

11	Describe your professional services offerings including but not limited to End user authentication configuration (using SAML, SSO Shibboleth, ADFS etc.).	<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. 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. 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. 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</p>
----	---	--

		<p>authentication unless required by policy, such as a second factor of authentication, providing a true clientless Single Sign-On capability. Fischer's self-service interfaces fully support SAML and CAS SSO login processes out of the box.</p>
--	--	---

12	Describe your professional services offerings including but not limited to Perform training, documentation and provide best practices.	Fischer Identity provides onsite training 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. Fischer provides an extensive amount of documentation covering every aspect of the product. Documentation is included in each build and can be downloaded from our FTP site. Given Fischer International Identity's history and experience, we are in a unique position to provide best practices recommendations at multiple levels. Fischer offers an implementation methodology that focuses on and exposes the best practices we've found over the years to be the path to a successful deployment. We've attached a white paper titled "Fischer Project Methodology" which explains in detail our approach to industry best practices.
13	Describe your professional services offerings including but not limited to Integration with upstream systems as documented within requirements; Configure workflows to map to existing business logic/process.	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. All interfaces are tested during UAT and prior to Go-Live.
14	Describe your professional services offerings including but not limited to Integration with downstream systems as documented within requirements.	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. All interfaces are tested during UAT and prior to Go-Live.

15	Describe your professional services offerings including but not limited to Review out-of-the box reporting and audit features. Design any recommended reports.	<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. Authorized users e.g. Administrators and Auditors can login into self-service to configure, run view and share the reports.</p>
16	Describe your professional services offerings including but not limited to Perform necessary decommission and transition steps for the legacy system.	Fischer will typically take a complete backup of the legacy system and provide a complete backup of the legacy solution to our clients. This includes any directory or database instances and/or server configuration files. Backups can also be done on virtual machines if the legacy deployment is utilizing that technology. We will also conform to any existing processes that are agreed upon during the initial project scope and contract process.

<p>17</p>	<p>Describe your training offerings for questions 18-21 including but not limited to the following:</p>	<p>Fischer offers 3 training methods that you can choose from that best fits the training needs of your organization:</p> <p>On Demand Web-Based LMS Courses Our web-based training courses covers the entire Fischer product, including but not limited to, comprehensive walkthroughs of configuring product features, IGA best practices, and troubleshooting. The web-based training is available 24 hours a day, 7 days a week. The content within the courses has closed captioning.</p> <p>Quarterly Training Workshops In this model, Fischer invites all of our customers to join our quarterly, collaborative training on the Fischer product.</p> <p>Dedicated Training Workshops The dedicated training workshop entails a member of the Fischer team to train your specific organization. Under this approach, a member of the Fischer team can perform training on-site at your location or we can host the dedicated training workshop at our headquarters location in Naples, Florida.</p> <p>Fischer also offer the Fischer Identity Guru Training Program for customer who would like to purchase additional training.</p> <p>Training Programs</p> <p>Location</p> <p>Fee</p> <p>Seats</p> <p>Description</p> <p>Online, self-paced program</p> <p>Virtual</p> <p>\$2,500.00</p> <p>Unlimited</p>
-----------	---	---

		<p>Unlimited Licensed Users and 24x7 access to Fischer's Guru training platform.</p> <p>Paradise Program</p> <p>Naples, FL</p> <p>\$4,500.00</p> <p>per Seat, max of 10</p> <p>Requires registration, fixed dates during the year and is open to all customers. Fischer would provide the lab environment necessary to commence training. Attendees would be required to bring a laptop to access the training lab. This training is limited to 10 attendees. There will be a schedule published annually for registration.</p> <p>Customized Training Tracks</p> <p>\$10,000.00</p> <p>5 full days of training at customer facilities. Fischer would provide the lab environment necessary to commence training. Attendees would be required to bring a laptop to access the training lab.</p> <p>General Overview & Implementation Training</p> <p>Customer premises max 10 attendees</p> <p>This course will provide participants with an overview of "How Fischer Works" and focus on how to implement an end to end solution Identity Governance & Administration solution leveraging the Fischer Identity Suite.</p> <p>Fischer Administration & Solution Mgt. Training</p> <p>Customer premises max 10 attendees</p>
--	--	---

		<p>This course will provide participants with a detailed review of the Administrative user interface as well as troubleshooting techniques and ongoing change control of your Fischer IGA solution.</p> <p>Infrastructure Training</p> <p>Customer premises</p> <p>max 10 attendees</p> <p>This course will provide participants with the know-how to install, configure and prepare the Fischer IGA Suite for Implementation and Production. This will include best practices around constructing your infrastructure as well as ongoing maintenance and monitoring solutions.</p> <p>Virtual Training Options</p> <p>"I Got This" wiki access only</p> <p>Virtual</p> <p>\$300.00</p> <p>per Seat</p> <p>Per user access to Fischer Central. This would provide an individual seat for Fischer's wiki to keep up to date with the latest training content in digital form.</p> <p>"Just print me the guides" PDF Guides</p> <p>N/A</p> <p>\$0.00</p> <p>NA</p> <p>If the customer chooses this model, Fischer will provide PDF of all current content for the trainee to review. Fischer will also offer access the assessments free of charge.</p>
--	--	---

		<p>Customized training can be extended to unlimited attendees for an additional \$5,000. Travel & Expense is not included in the Fee and would be billed separate.</p> <p>2 or more attendees from a single customer will result in a 20% discount per seat for the Paradise Program</p> <p>Attachment C : Training</p>
--	--	--

18	The recommended training plan for the initial implementation and ongoing support.	<p>Fischer Identity provides onsite training 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.</p> <p>All customer training and the associated material is created based on the specific design and functionality of the customer's solution. We utilize members of our Implementation and Solution Management teams to perform the training. Each team member has extensive knowledge of the Fischer product and have all facilitated training sessions with our customers. Fischer Product guides and solution documentation are provided as part of the training.</p>
19	Identify the roles requiring training and if there are separate training requirements for the technical systems support staff (including Help Desk, etc.) and administrators responsible for the day-to-day operation of the solution, functional staff, and super-users.	<p>Topic covered in basic training include: Managing Approvals; Adding Policies and Roles, Configuring Password management. Topic covered in advanced training include: Applying Patches and Managing Workflow Processes.</p> <p>For end users, Fischer offers "train the trainer" courses based on the modules being utilized. This approach allows your staff to train the user population as needed and typically reviews all end user interfaces your users will encounter.</p> <p>Fischer also offer the Fischer Identity Guru Training Program for customer who would like to purchase additional training.</p>
20	delivery approach for each training - is it offered/required onsite, offsite, web-based / CBT or remote	<p>Training can be held onsite, remotely through web-conference or at the Fischer Corporate Headquarters in Naples, FL. The training agenda is created for your solution, covering all areas your staff will need to understand how the product is integrated and deployed.</p>

21	Identify for each training option the number of hours, fees/pricing, and recommended timing	Fischer Identity provides onsite training 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.
22	Describe your product's solution integration including but not limited to Campus Single Sign On systems(SSO); Central Authentication System (CAS); Shibboleth (SAML); ADFS (SAML); MIT Kerberos	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. 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. 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. Fischer has developed a plugin for Active Directory which provides a seamless and true single sign-on experience for Windows desktop users. The SSO

		<p>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. Fischer's self-service interfaces fully support SAML and CAS SSO login processes out of the box. Fischer has an MIT Kerberos Connector.</p>
23	<p>Describe your product's solution integration including but not limited to LDAP systems like OpenLDAP, DSEE, ODSEE, PING LDSP or other implementation; Active Directory; Webservices/ESB integration with JBoss Fuse ESB, Mulesoft, WS02</p>	<p>Our product has different pieces that communicate with each other. Communication happens through web-services or through a replicated cache. The web-services calls are authenticated and signed. If any encrypted data is being sent over through a web-service, it is re-encrypted over the wire with previously shared asymmetric keys. If web-services calls are made over a non-secure network, we require that SSL is setup at the server level. The replicated cache uses JBoss Group technology to communicate. It is setup to use authentication and asymmetric encryption by default.</p>

24	Describe your product's solution integration including but not limited Support IAM portal functionality, either delivered or via APIs that can be used to build custom interfaces allowing for the creation/management of security questions, and password and MFA management. Microsoft Office 365 Suite; Azure AD; Google Suite for Education; AWS Control Tower;	Users can create/manage security questions, manage passwords and enroll/manage MFA using Fischer Self-Service Portal. Fischer offers connectors out of the box for Microsoft Office 365 Suite; Azure AD; Google Suite for Education, Blackboard, SQL databases, flat file and Windows Servers along with over another 100+ connectors in our library. Fischer's connectors have real time schema detection, so once the connected system is configured, you can refresh the connector and it will pull back all of the attributes from the system. Once a connector is in place, you can build out the workflow and map the attributes per your business requirements. Fischer can also build out additional connectors for our customers, often at no charge, as required. The Fischer Identity Connector Library is included with the solution.
25	Describe your product's solution integration including but not to Other systems including: ServiceNow; LMS (example, Blackboard, Canvas; Box; Salesforce; DocuSign	Fischer can integrate with all of the systems listed. Fischer has out-of-the box connectors for LDAP, Active Directory, PeopleSoft, Banner, Service Now, Microsoft Exchange, Microsoft SharePoint, Blackboard, Canvas, Box, SalesForce, Microsoft Office 365, Oracle Database, Microsoft SQL, MySQL, PostgreSQL Microsoft Windows Server, IBM AIX, Oracle Solaris, SUSE Linux Enterprise Server and Red Hat Enterprise Linux and supports flat file integration along with over another 100+ connectors in our library. Fischer's connectors have real time schema detection, so once the connected system is configured, you can refresh the connector and it will pull back all of the attributes from the system. Once a connector is in place, you can build out the workflow and map the attributes per your business requirements. Fischer can also build out additional connectors for our customers, often at no charge, as required. The Fischer Identity Connector Library is included with the solution.

<p>26</p>	<p>Describe your upgrade process (include communication points and lead-time notification). Identify if it is a re-implementation.</p>	<p>Our goal is 1 major release per year with 2 - 3 minor release and patches as necessary. We currently support 3 major release levels.</p> <p>Our versioning model consists of three numbers as: MAJOR.MINOR.PARTCH.</p> <p>MAJOR: it will be incremented based on a business decision, if the release is considered large, it will be incremented. MINOR: when new features are added to the product, the minor will be incremented. PATCH: any bug requiring a fix will trigger incrementing this value.</p> <p>For our hosted IaaS customers upgrades are required and performed by Fischer once per quarter, as needed. The maintenance window to perform Service Pack upgrades is typically 1 - 2 hours and they are applied during off-peak times during the early morning hours. During this time, Provisioning processes are suspended and users are presented with a prompt to indicate that the solution is currently undergoing maintenance when attempting to login to self-service to perform password resets, profile updates, etc. Hotfixes do not require a maintenance window or outage period. As with any upgrade, Fischer thoroughly tests all updates, prior to applying the update to client production environments.</p> <p>For our on-premises customers, upgrades and patches are available for download via our secure SFTP site. Availability of updates are communicated via an e-mail distribution list to our customers.</p> <p>We currently support 3 major releases.</p> <p>Prior to releasing any Service Pack, Fischer will send an e-mail notification to the client at least 30 days in advance of the scheduled upgrade. The notification specifies the date and time of when the upgrade will be deployed and the expected outage duration. If the client has a Test environment, the Service Pack will be deployed two weeks prior to upgrading the Production</p>
-----------	--	--

		<p>environment. This allows for adequate time for the client to test functionality, if they choose to do so.</p>
--	--	--

27	<p>Confirm there is no additional cost for product updates and that customizations and configurations made at UC should not be required to be rebuilt for each new software version.</p>	<p>Upgrades are completed at no cost. Fischer has an innovative "configuration" vs. "coding" approach that reduces the solution administration, increases sustainability and simplifies compliance and audit processes. The Fischer solution was purpose built to eliminate the need for proprietary protocols and complex scripting tools that require specialized expertise. Fischer has addressed the common shortfall in most identity management systems by designing the configuration into the system so setup is performed in point and click UI. To allow for more powerful configuration of lifecycle management and target system provisioning, Fischer provides our Workflow and Connectivity studio, an intuitive tool for workflow development and deployment with the power of full export, transformation & load functionality ETL. The workflows are not proprietary, instead they are stored and deployed XML objects.</p>
28	<p>Can upgrades be deferred and schedule as needed?</p>	<p>For our hosted IaaS customers upgrades are required and performed by Fischer once per quarter, as needed. The maintenance window to perform Service Pack upgrades is typically 1 - 2 hours and they are applied during off-peak times during the early morning hours. During this time, Provisioning processes are suspended and users are presented with a prompt to indicate that the solution is currently undergoing maintenance when attempting to login to self-service to perform password resets, profile updates, etc. Hotfixes do not require a maintenance window or outage period. As with any upgrade, Fischer thoroughly tests all updates, prior to applying the update to client production environments.</p> <p>For our on-premises customers, upgrades and patches are available for download via our secure SFTP site. Availability of updates are communicated via an e-mail distribution list to our customers.</p>

29	Confirm the following information is maintained for all maintenance service calls and made available to UC: nature of the deficiency, current status of the deficiency, action plans, dates, and times, expected and actual completion time, deficiency resolution information.	Fischer provides a web-based support portal for customers to report incidents, solution change requests, and inquiries. Fischer maintains the name, date, time, and priority of the deficiency/enhancement as well as the nature of the deficiency/enhancement, current status, action plans, dates, and times, expected and actual completion time, and resolution information. Customer have access in the support portal to view, comment and escalate if necessary.
30	List what source formats/repositories your product natively supports, including but not limited to:Flat-file, Java Database Connectivity (JDBC)/Open Database Connectivity (ODBC); Lightweight Directory Access Protocol (LDAP); Active Directory; SOAP; REST Web Services, PeopleSoft; Banner; Destiny1; ServiceNow; Microsoft Exchange, Microsoft SharePoint; G Suite, Salesforce, Microsoft Office 365 Suite; Oracle Database, Microsoft SQL, MySQL, PostgreSQL; Microsoft Windows Server, IBM AIX, Oracle Solaris, SUSE Linux Enterprise Server and Red Hat Enterprise Linux	Fischer can integrate with all of the systems listed. Fischer has out-of-the box connectors for LDAP, Active Directory, PeopleSoft, Banner, Service Now Microsoft Exchange, Microsoft SharePoint, Salesforce, Microsoft Office 365, Service Now, Oracle Database, Microsoft SQL, MySQL, PostgreSQL Microsoft Windows Server, IBM AIX, Oracle Solaris, SUSE Linux Enterprise Server and Red Hat Enterprise Linux and supports flat file integration along with over another 100+ connectors in our library. Fischer's connectors have real time schema detection, so once the connected system is configured, you can refresh the connector and it will pull back all of the attributes from the system. Once a connector is in place, you can build out the workflow and map the attributes per your business requirements. Fischer can also build out additional connectors for our customers, often at no charge, as required. The Fischer Identity Connector Library is included with the solution.
31	Does it support a complete data model that includes identity, application, account, entitlement and control data. .	Fischer Identity supports the eduPerson schema. In addition, has an extensible identity directory/repository schema that allows the solution to capture additional user-defined roles, attributes, and metadata, above and beyond the vendor's standard identity repository
32	Does it store both current and historical data	Fischer has a centralized identity directory/repository that supports multiple concurrent identity-related roles and affiliations and stores both current and historical data.
33	Does it provide a method to easily extend the schema to include additional, user-defined fields including binary data types.	Fischer Identity supports the eduPerson schema. In addition, has an extensible identity directory/repository schema that allows the solution to capture additional user-defined roles,

		attributes, and metadata, above and beyond the vendor's standard identity repository
34	Does it support the ability to link an identity to other identities to represent a relationship (e.g., manager-subordinate).	Relationship linking - the ability to link an identity to other identities to represent a relationship e.g., manager-subordinate is standard functionality.
35	Does it allow an organization to assign a sponsor to nonemployee user accounts such as contractors - this pseudo-manager would act as an approver for workflows, access reviews and certifications, and so on.	Each resource requested can have a "Sponsor" assigned to it that is responsible for the user similar to how a Manager would be responsible for an employee. The sponsor can be an approver for workflows, access reviews and certifications, and so on.
36	If the answer to 35 is yes, does it detect orphaned/unowned accounts and initiate a workflow to reassign a new pseudo-manager or take some other corrective action.	Real-time monitoring can be implemented to catch any violations to access and take immediate action. This can initiate an approval processes, removal of access, or notification to appropriate users. If approvals are used, they can be used to remove access or retain access based on the approval flow outcome.
37	Does it Provide the ability to detect corrupt or truncated data coming from an authoritative source and trigger corrective action.	Fischer has workflow rules that can detect corrupt or truncated data coming from an authoritative source and trigger corrective action.
38	Does your provide out-of-the-box identity life cycle management support for multiple types of users, within different constituencies.	This is standard functionality for Fischer. Multiple concurrent constituency types are supported via Identity Lifecycle Management ILM processes, including, faculty, staff, student, contractor, affiliate, applicant, alumni, and other user-defined constituency types, or roles out-of-the-box.
39	Does your solution allow an organization to represent multiple organizational relationships with a single identity.	Fischer has a centralized identity directory/repository that supports multiple concurrent identity-related roles and affiliations and stores both current and historical data.

40	How does your solution manage identity matching? Does your solution provide an ability to manually match or splut identities generated from multiple authoritative sources?	Using our powerful identity matching, if the same identity came from separate sources of authority, the matching system would pause the provisioning activity until the match could be resolved. Then independent processing of the new authoritative identity record would continue. Additionally, the Fischer Identity solution isolates the attribute policy mapping independent from the managed system connectors so that we can simultaneously pull identity information from multiple authoritative sources. We call this process staging with delta processing. The sources can be of multiple technologies and we export adds, changes and deletes from the SoAs and consolidate them into identity events.
41	Does your solution support the ability to have one identity with multiple personas.	Fischer has a centralized identity directory/repository that supports multiple concurrent identity-related roles and affiliations and stores both current and historical data.
42	Describe the mechanism for reconciling connected systems (whether authoritative or target) with the identity repository.	The Fischer solution leverages its ETL engine in order to do reconciliation of data between sources of truth and other targets systems. This can be done in real-time during the processing of the record from the source of truth, or as a secondary process to reconcile the data during a scheduled process. You are capable of reconciliation not only from the source of truth, but any target system that Fischer is able to manage.
43	Does your solution provide the ability to reconcile attribute conflicts when the same attribute is sourced from connected systems.	Fischer Connectors are bidirectional for the purpose of reconciliation and attestation. Fischer can utilize our ETL engine to create processes for reconciliation against any target that Fischer is managing. In scenarios where there are multiple SoAs, The client determines which SoA source is preferred for a given attribute and a workflow is created. If there is a conflict, the attribute from the preferred SoA is used.
44	Does your solution provide a mechanism for not only aggregating identity data, but storing the data in a normalized format in the repository.	Fischer Connectors are bidirectional for the purpose of reconciliation and attestation. Fischer can utilize our ETL engine to create processes for reconciliation against any target that Fischer is managing. In scenarios where there are multiple SoAs, The client determines which SoA source is preferred for a given attribute and a workflow is

		created. If there is a conflict, the attribute from the preferred SoA is used.
45	Does your solution provide support for modifying user identifiers for connected systems.	Fischer Connectors are bidirectional for the purpose of reconciliation and attestation. Fischer can utilize our ETL engine to create processes for reconciliation against any target that Fischer is managing. In scenarios where there are multiple SoAs, The client determines which SoA source is preferred for a given attribute and a workflow is created. If there is a conflict, the attribute from the preferred SoA is used.
46	Does your solution support the ability to detect changes in a source system's schema and create new attributes as required.	Fischer can utilize our ETL engine to create processes for reconciliation against any target that Fischer is managing. In scenarios where there are multiple SoAs, The client determines which SoA source is preferred for a given attribute and a workflow is created. If there is a conflict, the attribute from the preferred SoA is used.
47	Does your solution assign a unique identifier to each identity.(A unique ID should not be confused with a login ID or account alias)	<p>The Fischer solution is usually configured to assign a persistent unique identifier. Depending on the configuration requirements, existing unique identifiers, and source of authority processing, the unique ID may be configured to align with one or more of these source systems. Internally, Fischer maintains it's own GUID to ensure that changes to unique ID or other need for persistent record identification is maintained.</p> <p>Fischer can create this unique identifier in any format you require using Fischer's data mapper. The data mapper is where the business logic is scripted and data is validate and manipulated.</p>

48	Does your solution support both full-batch processing (the entire identity record is replaced) and change-log batch processing (only affected identity attributes are updated).	Fischer's solution supports both full-batch processing and and change-log batch processing. Workflows can be designed in multiple ways to fit the customer's specific architectural and business requirements with both "real time" push and batch processing pull capabilities depending on system requirements. Triggers and SPML BEIS messages are supported for real-time event detection. In batch processing, Fischer automatically records the state of the export and can perform subsequent "delta" exports where only changed records are processed. Data synchronization processes are managed as Workflows built with the Fischer Studio. When changes are detected, either by push or pull, the process will determine what has changed added/modified/deleted and pass that change type to downstream process workflows and the provisioning engine. Workflows can be tied together and success and failure workflow processing initiated as the need dictates. When multiple sources of record are required to build a complete view of the identity's access requirements, Fischer architecture supports a "staging" process where changes are recognized and multiple sources combined and sent to the provisioning engine for full and accurate provisioning.
49	Does your solution provide a web- or client-based interface that allows individual users, or delegated administrators on behalf of users, to trigger identity life cycle events.	Fischer Self-Service Access Request feature enables users to request access or attribute changes and initiate the approval process, if required, through an intuitive, responsive web UI application for desktop, tablet, and mobile devices. Users are presented with only the resources and profile attributes that they are authorized to select, view or modify, ensuring that the "principle of least privilege" is always enforced. All events are fully audited, from request to approval. Authorized users may also request access on behalf of other users, make changes to existing access and remove access or even create users who don't appear in the sources of authority, such as contractors or vendors.

50	Does your solution provide event-driven identity life cycle event management in real-time or near-real-time processing.	Fischer provides end to end life cycle management of all user types. Initiating the user object inception from multiple source systems where logical rules and identity matching are configured to maintain continuity between sources of truth. User object changes are detected and evaluated for provisioning, deprovisioning, attribute updates and access control decisions including both accounts and permissions entitlements.
51	Can it support both start and end future dating.	Fischer supports both "Account-EndDate" and "Account-StartDate" options, or what we call a future dated transactions that will automatically provision or de-provision access on the set date. This date can be set at initial provisioning time and can be extended or decreased throughout the life-cycle of the identity.
52	Does it allow the ability to view and manage all applications, policies, roles, entitlements, accounts and attributes associated with an identity object.	<p>The Fischer solution provide the management of identity records for both person and non-person accounts like the club accounts example. The security model combined with the sponsorship feature allows for refined administration of these non-person accounts. Delegated administration is accomplished with the security profile and authorization based on attribute conditions and rules configurations.</p> <p>Fischer provides a native security model empowering our customers to define a security hierarchy within the IAM application. Users and associated authorizations can be defined in a granular fashion. Attribute based access control is available to qualify users for delegated administration or approval authorizations based on particular attributes. Role based Access Control is also available. Each group is provided a set of permissions pertaining to what level of action they can take against the identity or identities they are authorized to administer. This functionality extends across the entire product from administration to self-service interfaces.</p>

53	<p>Does it support views including identity-centric, application-centric, policy- or role- centric, and entitlement- or account-centric views. Does solution allow users to delegate some or all of their access.</p>	<p>The Fischer solution provide the management of identity records for both person and non-person accounts like the club accounts example. The security model combined with the sponsorship feature allows for refined administration of these non-person accounts. Delegated administration is accomplished with the security profile and authorization based on attribute conditions and rules configurations.</p> <p>Fischer provides a native security model empowering our customers to define a security hierarchy within the IAM application. Users and associated authorizations can be defined in a granular fashion. Attribute based access control is available to qualify users for delegated administration or approval authorizations based on particular attributes. Role based Access Control is also available. Each group is provided a set of permissions pertaining to what level of action they can take against the identity or identities they are authorized to administer. This functionality extends across the entire product from administration to self-service interfaces.</p>
54	<p>Does it provide a registration portal that allows the individual to create and manage a user account or request access as necessary.</p>	<p>Fischer Self-Service Access Request feature enables users to request access or attribute changes and initiate the approval process, if required, through an intuitive, responsive web UI application for desktop, tablet, and mobile devices. Users are presented with only the resources and profile attributes that they are authorized to select, view or modify, ensuring that the "principle of least privilege" is always enforced. All events are fully audited, from request to approval. Authorized users may also request access on behalf of other users, make changes to existing access and remove access or even create users who don't appear in the sources of authority, such as contractors or vendors.</p>

55	How does your solution handle password recovery? Are options available for users to recover passwords through challenge response, secondary (external) email, SMS, or MFA? -	Users have a simple and consistent self-service UI that does everything from password reset to profile management, including help desk functionality and resource requests and approvals. Users can manage their identity profile and reset and synchronize passwords across virtually all systems. User authentication is performed using the traditional question/answer approach, SMS-based one-time validation codes, or both to gain the added security of 2- factor authentication. Federated Single Sign-On Provides a login-free experience to your users when accessing web and SaaS applications while protecting users from attempts to intercept personal login credentials or being victimized by "man in the middle attacks." Federation configuration management is greatly simplified through the use of a graphical interface, eliminating the need to manually edit complex XML files.
56	Does it support the ability to create a random password for a user account.	Yes, we can generate a random password so users can use it to set their own password utilizing the user portal. However, the preferred method is to send the user an authorization code that is used when they first visit the kiosk or to pre-populate answers to questions for the user. This can include any information you have available for a user, such as birth date, last 4 of the social security number, home phone number, etc.

57	Does the solution allow the ability to view and manage all applications, policies, roles, entitlements, accounts and attributes associated with an identity object.	<p>The Fischer solution provide the management of identity records for both person and non-person accounts like the club accounts example. The security model combined with the sponsorship feature allows for refined administration of these non-person accounts. Delegated administration is accomplished with the security profile and authorization based on attribute conditions and rules configurations.</p> <p>Fischer provides a native security model empowering our customers to define a security hierarchy within the IAM application. Users and associated authorizations can be defined in a granular fashion. Attribute based access control is available to qualify users for delegated administration or approval authorizations based on particular attributes. Role based Access Control is also available. Each group is provided a set of permissions pertaining to what level of action they can take against the identity or identities they are authorized to administer. This functionality extends across the entire product from administration to self-service interfaces.</p>
58	Does the solution support views including identity-centric, application-centric, policy- or role- centric, and entitlement- or account-centric views.	<p>The Fischer solution provide the management of identity records for both person and non-person accounts like the club accounts example. The security model combined with the sponsorship feature allows for refined administration of these non-person accounts. Delegated administration is accomplished with the security profile and authorization based on attribute conditions and rules configurations.</p> <p>Fischer provides a native security model empowering our customers to define a security hierarchy within the IAM application. Users and associated authorizations can be defined in a granular fashion. Attribute based access control is available to qualify users for delegated administration or approval authorizations based on particular attributes. Role based Access Control is also available. Each group is provided a set of permissions pertaining to what level of action they can take against the identity or identities they are authorized to administer. This functionality extends across the entire product from administration to self-service interfaces.</p>

59	Does it provide a registration portal that allows the individual to create and manage a user account or request access as necessary.	Fischer Self-Service Access Request feature enables users to request access or attribute changes and initiate the approval process, if required, through an intuitive, responsive web UI application for desktop, tablet, and mobile devices. Users are presented with only the resources and profile attributes that they are authorized to select, view or modify, ensuring that the "principle of least privilege" is always enforced. All events are fully audited, from request to approval. Authorized users may also request access on behalf of other users, make changes to existing access and remove access or even create users who don't appear in the sources of authority, such as contractors or vendors.
60	Does the solution enforce password policies.	Fischer's Password Management Solution includes the ability to enforce all typical password policy constraints including: password expiration, password length, password history, complexity and restrictions against dictionary words, repeating characters, sequential characters and user of full or partial names, etc.
61	Does it include an entitlement catalog that allows you to track and define entitlement dependencies	The Request Access feature in the Fischer Self-Service application serves as the Entitlements Management / Catalog for Fischer identity. Fischer Self-Service Access Request feature enables users to request access or attribute changes and initiate the approval process, if required, through an intuitive, responsive web UI application for desktop, tablet, and mobile devices. Users are presented with only the resources and profile attributes that they are authorized to select, view or modify, ensuring that the "principle of least privilege" is always enforced. All events are fully audited, from request to approval. Authorized users can create new users, add resources and entitlement, provides for resource and entitlement adds, changes and removal where authorized users can request resource access and entitlements either by user or by resource. These requests can be processed and granted if the policy allows immediately or sent through the approval system. "One-off" or override of birthright access can be requested and access periods configured and maintained for time-bound access control and automatic access removal or deprovisioning.

		<p>This can be done for a single user or in bulk through the UI.</p>
62	<p>Does it provide a method to easily extend the schema to include additional, user-defined fields</p>	<p>Fischer Identity supports the eduPerson schema. In addition, has an extensible identity directory/repository schema that allows the solution to capture additional user-defined roles, attributes, and metadata, above and beyond the vendor's standard identity repository</p>

63	Explain the entitlement catalog schema including but not limited to the following metadata fields:	<p>The Request Access feature in the Fischer Self-Service application serves as the Entitlements Management / Catalog for Fischer identity. Fischer Self-Service Access Request feature enables users to request access or attribute changes and initiate the approval process, if required, through an intuitive, responsive web UI application for desktop, tablet, and mobile devices. Users are presented with only the resources and profile attributes that they are authorized to select, view or modify, ensuring that the "principle of least privilege" is always enforced. All events are fully audited, from request to approval. Authorized users can create new users, add resources and entitlement, provides for resource and entitlement adds, changes and removal where authorized users can request resource access and entitlements either by user or by resource. These requests can be processed and granted if the policy allows immediately or sent through the approval system. "One-off" or override of birthright access can be requested and access periods configured and maintained for time-bound access control and automatic access removal or deprovisioning. This can be done for a single user or in bulk through the UI.</p>
----	--	---

64	<p>Explain the entitlement catalog schema including but not limited to the following metadata fields: Entitlement technical name; Entitlement display name; Technical description; Plain-language business description; Entitlement owner; Entitlement category (entitlement, role, account, privileged account and so on)</p>	<p>The Request Access feature in the Fischer Self-Service application serves as the Entitlements Management / Catalog for Fischer identity. Fischer Self-Service Access Request feature enables users to request access or attribute changes and initiate the approval process, if required, through an intuitive, responsive web UI application for desktop, tablet, and mobile devices. Users are presented with only the resources and profile attributes that they are authorized to select, view or modify, ensuring that the "principle of least privilege" is always enforced. All events are fully audited, from request to approval. Authorized users can create new users, add resources and entitlement, provides for resource and entitlement adds, changes and removal where authorized users can request resource access and entitlements either by user or by resource. These requests can be processed and granted if the policy allows immediately or sent through the approval system. "One-off" or override of birthright access can be requested and access periods configured and maintained for time-bound access control and automatic access removal or deprovisioning. This can be done for a single user or in bulk through the UI.</p>
65	<p>Does it provide an administrative dashboard for monitoring the progress of onboarding applications into the entitlement repository.</p>	<p>Fischer allows for authorized user to see all events that are processed through the self-service portal. Here they can filter only the events that they wish to review. This includes onboarding for applications and entitlements.</p>
66	<p>Does it provide a tool that walks an administrator through the steps required to onboard applications into the entitlement catalog.</p>	<p>Fischer's Request Access Feature, provides a UI and step-by-step instructions required to onboard applications into the Request Access entitlements list.</p>
67	<p>Describe the mechanism for end users to claim the accounts that belong to them.</p>	<p>Fischer Account Claim is highly configurable including allowing claim and activation by verifying user identity with a random one-time use authorization code and/or by validation of pre-populated information from a source of record. The claim information can be sent to the users during Source of Authority processing and their account credentials sent at that time or revealed during account claim. User can login to the Self-Service UI and claim the accounts that belong to them.</p>

68	Describe how fulfillment connectors are used or how read- only connectors to discover entitlements in applications are handled	Fischer can use it's connectors to discovery entitlements within applications where connectors are available. This allows Fischer to import those entitlements and make them available to be associated with users for provisioning, deprovisioning and auditing. Fischer can accept CSV file imports for the purposes of importing/discovering of entitlements.
69	Describe the ability to consume and understand entitlements from applications with complex authorization models.	As needed, Fischer will deploy the solution with 'automation' workflows. In order to monitor new entitlements, Fischer will utilize the Extraction, Transformation, Load ETL capabilities of our workflow studio. Automation workflows will pull entitlements from a system on a scheduled basis, any new entitlements can trigger a workflow and notification process to coordinate the work required to enrich the entitlement with metadata. Schedules can be setup to run minutes, hours, days, weeks, etc.
70	Does it correlate disparate user accounts and entitlements with a single identity	Authorized users are allowed to statically link an account with an identity as well as allowing Fischer to dynamically link account and entitlements.
71	Describe methods for matching an identity to its disparate applications, user accounts and entitlements, including but not limited to Static linking: User interface that allows administrators to permanently link an identity to an account Dynamic linking: Conditional or attribute-based rules that match an identity to a user account and entitlements	Authorized users are allowed to statically link an account with an identity as well as allowing Fischer to dynamically link account and entitlements.

Table 4 Identity Governance Part B

1	Does it allow reviewers to view access by user, resource, role, or by account or entitlement and to certify access to entitlements, roles, resources or related items.	<p>You can review access for users in the context of access policies, accounts and entitlements. You can "allow", "remediate", or "remove" access during the review process. 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 Fischer compliance system supports powerful configuration beginning with the definition of Chain of Trust made up of certifiers, or users selected statically specific user or dynamically logical expression. Certifiers can be assigned to groups of users for the purposes of attestation reviews. The Chain of Trust is assigned to Compliance jobs where policies, resources accounts and/or entitlements, and systems are configured for assessment and/or review by the Chain of Trust and optionally parallel technical review. Certifiers can "allow", "remediate", or "remove" access during the review process. Compliance assessments can be executed on a scheduled basis to find and report all access control policy violations and present audit controllers with remediation options as well as override options, including access certification.</p>
2	Describe ability of the reviewer to download the certification file as a spreadsheet and complete it offline.	The Certification file can be downloaded as a spreadsheet and reviewed offline.

3	Workflow	Serial, parallel, and hierarchical approval routing with escalations, response time out, reassignment, overrides, exception handling, and delegation all supported. Conditional workflow processing as part of the workflow engine, where workflow steps can be dynamically determined by the outcome of other workflow steps is configurable.
4	How does the solution kick of a remediation event if the reviewer determines that an entitlement is inappropriate,	A workflow with email notification and approval including comments can be tied to a remediation event.

5	<p>Does solution support a challenge period that gives end users a chance to contest a pending remediation resulting from an access certification.</p>	<p>You can review access for users in the context of access policies, accounts and entitlements. You can "allow", "remediate", or "remove" access during the review process. 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 Fischer compliance system supports powerful configuration beginning with the definition of Chain of Trust made up of certifiers, or users selected statically specific user or dynamically logical expression. Certifiers can be assigned to groups of users for the purposes of attestation reviews. The Chain of Trust is assigned to Compliance jobs where policies, resources accounts and/or entitlements, and systems are configured for assessment and/or review by the Chain of Trust and optionally parallel technical review. Certifiers can "allow", "remediate", or "remove" access during the review process. Compliance assessments can be executed on a scheduled basis to find and report all access control policy violations and present audit controllers with remediation options as well as override options, including access certification.</p>
---	--	--

6	<p>How does Solution provide configurable account creation policies that dictate the following: required attributes; password policies; required criteria for account to be created; format of the account name; determination if the user account already exists on the target system; containers where the account will be created in the application</p>	<p>Fischer has the strongest and most robust provisioning solution in the market. 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 can dictate the following: required attributes, password policies, required criteria for account to be created, format of the account name, containers where the account will be created in the application, and determines if the user account already exists on the target system. Fischers deprovisioning policies allow for deletion, disabling or suspension of accounts. Placement policy can define inactive account location as well as define account retention policies. Fischer can qualify / disqualify users with specific parts of their overall roles. 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 is typically controlled by affiliations and roles. Fischer can not only handle multiple Sources of Record but also multiple affiliations.</p>
---	---	---

7	Does solution provide configurable account deletion policies that allow for deletion, disabling or suspension of accounts.	Fischers deprovisioning policies allow for deletion, disabling or suspension of accounts. Placement policy can define inactive account location as well as define account retention policies. Fischer can qualify / disqualify users with specific parts of their overall roles. 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 is typically controlled by affiliations and roles. Fischer can not only handle multiple Sources of Record but also multiple affiliations
8	What is the placement policy that defines inactive account location.	Placement policy can define inactive account location as well as define account retention policies. Fischer can qualify / disqualify users with specific parts of their overall roles. 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 is typically controlled by affiliations and roles. Fischer can not only handle multiple Sources of Record but also multiple affiliations.

9	Define solution's account retention policies.	Fischers deprovisioning policies allow for deletion, disabling or suspension of accounts. Placement policy can define inactive account location as well as define account retention policies. Fischer can qualify / disqualify users with specific parts of their overall roles. 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 is typically controlled by affiliations and roles. Fischer can not only handle multiple Sources of Record but also multiple affiliations.
---	---	--

10	Describe how solution transforms data and events which include account creation and deletion into the proper format for a given target system.	Fischer has the strongest and most robust provisioning solution in the market. 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 can dictate the following: required attributes, password policies, required criteria for account to be created, format of the account name, containers where the account will be created in the application, and determines if the user account already exists on the target system. Fischers deprovisioning policies allow for deletion, disabling or suspension of accounts. Placement policy can define inactive account location as well as define account retention policies. Fischer can qualify / disqualify users with specific parts of their overall roles. 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 is typically controlled by affiliations and roles. Fischer can not only handle multiple Sources of Record but also multiple affiliations.
11	Does it allow the ability to associate a single identity with multiple user accounts within a single application.	Fischer Identity meets these requirements.

12	How does solution add (provision), modify and delete (deprovision) user accounts, and also synchronize identity attributes, entitlements, and data from an authoritative source to target systems.	Fischer can add provision, modify and delete deprovision user accounts and synchronize identity attributes, entitlements, and data from an authoritative source to target systems. Data synchronization processes are managed as Workflows built with the Fischer Studio. Once a connector is in place, you can build out the workflow and map the attributes per your business requirements.
13	Does solutuion support unidirectional and bidirectional data synchronization.	Fischer Connectors are bidirectional for the purpose of reconciliation and attestation. Fischer can utilize our ETL engine to create processes for reconciliation against any target that Fischer is managing. In scenarios where there are multiple SoAs, The client determines which SoA source is preferred for a given attribute and a workflow is created. If there is a conflict, the attribute from the preferred SoA is used.
14	Does it allow mapping of attribute data between the identity repository and managed systems (authoritative and target).	Fischer's connectors have real time schema detection, so once the connected system is configured, you can refresh the connector and it will pull back all of the attributes from the system. Once a connector is in place, you can build out the workflow and map the attributes per your business requirements.

15	Does it support staged deprovisioning, for example disable account and delete after a defined period of time.	Yes, Fischer supports disabling identities or deleting them. The typical scenario is to disable for an extended period of time, then delete. Each system disables accounts differently. Depending on the system, Fischer would take the appropriate syntactically correct actions.
16	Does solution provide a documented software development kit (sdk) with specific example code that allows organization to build custom connectors.	We do not have an SDK. However, we do provide detailed documentation on how to build your own connectors including the required java libraries and classes and Fischer can also build out additional connectors for our customers, often at no charge, as required.
17	Does solution support the ability to swap fulfillment mechanisms without needing to create a new representation of the target resource in the entitlements repository.	Fischer has a data mapper where the business logic is scripted and data is validate and manipulated. Once a connector is in place, you can build out the workflow and map the attributes per your business requirements. Out of the box library workflows can be used as a starting point to add company specific logic.
18	Does solution offer flexibility to map individual provisioning operations to different connectors.	We do not have an SDK. However, we do provide detailed documentation on how to build your own connectors including the required java libraries and classes and Fischer can also build out additional connectors for our customers, often at no charge, as required.

19	How does solution connect to multiple target systems.	<p>The Fischer solution leverages its ETL engine in order to do reconciliation of data between sources of truth and other targets systems. This can be done in real-time during the processing of the record from the source of truth, or as a secondary process to reconcile the data during a scheduled process. You are capable of reconciliation not only from the source of truth, but any target system that Fischer is able to manage.</p> <p>Fischer Connectors are bidirectional for the purpose of reconciliation and attestation. Fischer can utilize our ETL engine to create processes for reconciliation against any target that Fischer is managing. In scenarios where there are multiple SoAs, The client determines which SoA source is preferred for a given attribute and a workflow is created. If there is a conflict, the attribute from the preferred SoA is used.</p>
----	---	--

20	<p>Describe support out-of-the box connectivity with common formats, which must be able to write data to include but not limited to the following: Flat-file; Java Database Connectivity (JDBC)/Open Database Connectivity (ODBC); Lightweight Directory Access Protocol (LDAP); Active Directory; SOAP and REST Web Services; PeopleSoft, Banner, Destiny1; ServiceNow, EverBridge; Microsoft Exchange, Microsoft SharePoint; G Suite, Salesforce, Microsoft Office 365 and ServiceNow; Oracle Database, Microsoft SQL, MySQL, PostgreSQL; Microsoft Windows Server, IBM AIX, Oracle Solaris, SUSE Linux Enterprise Server and Red Hat Enterprise Linux; Shibboleth (SAML); Central Authentication System (CAS); System for Cross-Domain Identity Management (SCIM) 2.0 requests; External Logging Systems (similar to Splunk and ELK)</p>	<p>Fischer can integrate with all of the systems listed. Fischer has out-of-the box connectors for LDAP, Active Directory, PeopleSoft, Banner, Service Now Microsoft Exchange, Microsoft SharePoint, SalesForce, Microsoft Office 365, Service Now, Oracle Database, Microsoft SQL, MySQL, PostgreSQL Microsoft Windows Server, IBM AIX, Oracle Solaris, SUSE Linux Enterprise Server and Red Hat Enterprise Linux and supports flat file integration along with over another 100+ connectors in our library. Fischer's connectors have real time schema detection, so once the connected system is configured, you can refresh the connector and it will pull back all of the attributes from the system. Once a connector is in place, you can build out the workflow and map the attributes per your business requirements. Fischer can also build out additional connectors for our customers, often at no charge, as required. The Fischer Identity Connector Library is included with the solution.</p> <p>Attached Files : Fischer Identity Connectors.pdf</p>
21	<p>Does solution have ability to request access via a single page or free-form vs a sequential wizard-driven approach.</p>	<p>Yes, Fischer Identity meets these requirements.</p>

22	Does solution allow requesters to add new access, modify existing access or remove existing access.	Yes, Fischer Self-Service Access Request feature enables users to request access or attribute changes and initiate the approval process, if required, through an intuitive, responsive web UI application for desktop, tablet, and mobile devices. Users are presented with only the resources and profile attributes that they are authorized to select, view or modify, ensuring that the "principle of least privilege" is always enforced. All events are fully audited, from request to approval. Authorized users may also request access on behalf of other users, make changes to existing access and remove access or even create users who don't appear in the sources of authority, such as contractors or vendors.
23	Does it allow a requester to request access to entitlement objects, role, application and account objects.	Yes, Fischer Identity allows a requester to request access to entitlement objects, role, application and account objects.
24	Does it provide an e-commerce-like shopping cart experience that allows requesters to add entitlements to a shopping cart, view entitlements in the cart, remove entitlements in the cart and check ou	Yes, Fischer Identity meets these requirements.
25	Does it have ability for a user or authorized user to view their own profile and associated entitlements	Yes, Fischer provides the ability for a user or an authorized user to view their own profile and associated entitlements.

26	Does it allow user to personalize the access request user interface (UI).	Yes, Fischer Identity can be configured to utilize complete UC System branding and login page design. Fischer can provide CSS, JavaScript and XHTML capabilities but these items are considered billable if performed by Fischer.
27	Does it provide administrative tools that allow personalization of the look and feel of the interface, add attributes, customize page layouts and so on at a global level.	Fischer provides the ability for a user or an authorized user to view their own profile and associated entitlements. Fischer Identity can be configured to utilize complete UC System branding and login page design. Fischer can provide CSS, JavaScript and XHTML capabilities but these items are considered billable if performed by Fischer.
28	Does it provide a search engine that allows requesters to search the entitlements repository	The entitlement catalog is fully searchable and available entitlements are filtered by role, group or attributes of that logged in user. While Fischer can 'transfer' access of accounts to another user, Fischer does not recommend copying user access from one user to another, but this can be done using a workflow. In general, we advise and would much rather implement the correct roles and policies that govern access so when a user is entered they receive the appropriate access based on their roles and attributes.
29	Can it assist requestors by making entitlement suggestions, filtering the entitlements according to role, group, or other filter.	The entitlement catalog is fully searchable and available entitlements can be filtered by role, group or attributes of that logged in user.

30	Does it allow requestor to compare and copy access from other users that are in a similar role or peer group.	While Fischer can 'transfer' access of accounts to another user, Fischer does not recommend copying user access from one user to another, but this can be done using a workflow. In general, we advise and would much rather implement the correct roles and policies that govern access so when a user is entered they receive the appropriate access based on their roles and attributes.
31	Does it have an administrative interface that provides ability to request access to an entitlement for multiple users	You can request access to an entitlement for multiple users.
32	Do approvers have the ability to delegate some or all of their authority to another user.	Yes, Approval delegation is configurable and supported in the Self-Service application including managed availability.
33	Is access request status, workflow steps and approvers visible to the requester, the recipient, approvers and observers (if applicable) as configured by organizational policy.	Access request status, workflow steps and approvers are be visible to the requester, the recipient, approvers and observers if applicable as configured by organizational policy.
34	Does it allow requests that have been submitted for approval, but not yet processed, to be canceled or modified.	Access requests that have been submitted for approval, but not yet processed, can be canceled or modified.
35	Does it allow requests to be submitted using a pre-defined template.	Requests can be submitted using pre-defined workflows.

36	Does it allow ability to define and configure the treatment of high-risk requests by automatically denying, sending notifications, requiring justification, requiring effective dates, and escalation of approval.	The Self-Service application provides the interface for the requests and approvals and management of their workflows and lifecycle. Approvals can be configured with unlimited approvers in all common configurations; quorum, parallel, serial, etc. Notifications are naturally built into the system for all affected users. Approval delegation is configurable and supported in the Self-Service application including managed availability. Custom attributes can be configured for the approval process and requests can be returned for additional information or clarification to any user in the request and approval chain. The approval configurations are also available to the Fischer Workflow and Connectivity Studio allowing for powerful integration with the automated systems, whether driven off of a button in the Self-Service profile or as part of the export, import or provisioning process
37	Can access requests support requesting effective dates for start and end of access.	Fischer supports both "Account-EndDate" and "Account-StartDate" options, or what we call a future dated transactions that will automatically provision or de-provision access on the set date. This date can be set at initial provisioning time and can be extended or decreased throughout the life-cycle of the identity.

38	Requests should be blocked if dependencies are missing.	Fischer supports both "Account-EndDate" and "Account-StartDate" options, or what we call a future dated transactions that will automatically provision or de-provision access on the set date. This date can be set at initial provisioning time and can be extended or decreased throughout the life-cycle of the identity.
39	Does solution run on common platforms/application servers and support common data repositories including but not limited to Platforms - Windows and Linux Application Servers - Apache Tomcat and IIS Data Repositories - Active Directory or Database (Oracle or MSSQL)	<p>The Fischer Identity Suite is capable of running on Windows 2008 R2 or later. The application is a Java based web application which uses apache tomcat as its application server. The Fischer Identity Suite supports Active Directory, SOAP, REST, and SQL. The Fischer Application requires a Database and LDAP Active Directory in order to install the Fischer application suite.</p> <p>Fischer uses an agnostic approach for our environment. Allowing you to choose which platform, database, directory, etc. can be used. We support both Windows and UNIX installations. We support MSSQL, Postgres, Oracle databases. We also support any v3 compliant LDAP as the directory.</p>

40	Does solution allow easy installation in a predefined configuration that minimizes initial deployment time, such as a soft appliance.	Fischer provides automated installers for each component and updates/upgrades for each of the platforms Windows, UNIX/Linux. These include software installation, directory and database configuration. Fischer also supports AWS installation.
41	Does solution have ability to install all core components through an intuitive wizard.	Fischer provides automated installers for each component and updates/upgrades for each of the platforms Windows, UNIX/Linux. These include software installation, directory and database configuration. Fischer also supports AWS installation.
42	User Interface	Roles can be designed and modeled using the administrative user interface. This includes the ability to build conditions and rules from identity attributes to be used for role qualification. Rules and conditions can be modeled to show what users 'would' qualify based on the changes and then allow administrators to accept or reject those changes based on the results of their modeling.

43	Describe all administrative functions accessible via a web interface.	<p>The Fischer administrative UI provides all the screens necessary to configure and manage profiles, approvals, workflow schedules, compliance, auditing, reporting, etc. and is a separate interface from the Fischer self-service UI.</p> <p>Fischer Identity can be configured to utilize complete UC System branding and login page design. Fischer can provide CSS, JavaScript and XHTML capabilities but these items are considered billable if performed by Fischer.</p>
44	Describe ability to provide suggestions for assigning roles, policies, entitlements and access in all user interfaces.	The entitlement catalog is fully searchable and available entitlements can be filtered by role, group or attributes of that logged in user.
45	Does it allow organizations to define policies with the ability to trigger a workflow.	Fischer supports both "Account-EndDate" and "Account-StartDate" options, or what we call a future dated transactions that will automatically provision or de-provision access on the set date. Fischer utilizes its provisioning engine to monitor changes that impact downstream accounts. Changes to an identity in the Source of Record or events initiated within the Fischer Self-Service User Interface, can automatically trigger events to make changes to target resources or trigger other workflow actions.

46	Configuration & Development	<p>Fischer has an innovative "configuration" vs. "coding" approach that reduces the solution administration, increases sustainability and simplifies compliance and audit processes. The Fischer solution was purpose built to eliminate the need for proprietary protocols and complex scripting tools that require specialized expertise. Fischer has addressed the common shortfall in most identity management systems by designing the configuration into the system so setup is performed in point and click UI. To allow for more powerful configuration of lifecycle management and target system provisioning, Fischer provides our Workflow and Connectivity studio, an intuitive tool for workflow development and deployment with the power of full export, transformation & load functionality ETL. The workflows are not proprietary, instead they are stored and deployed XML objects.</p>
----	-----------------------------	---

47	Does solution provide version control (tracking and recording changes to the environment over time)assign version, bundle changes together and move them between different environments.	<p>Our versioning model consists of three numbers as: MAJOR.MINOR.PARTCH.</p> <p>MAJOR: it will be incremented based on a business decision, if the release is considered large, it will be incremented.</p> <p>MINOR: when new features are added to the product, the minor will be incremented.</p> <p>PATCH: any bug requiring a fix will trigger incrementing this value.</p> <p>We currently support 3 major releases.</p> <p>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.</p> <p>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. We store a record of any accounts or entitlements associated with a user, including group memberships. This information is also stored within our audit database. Additionally, we can take snapshots of target systems account and group memberships which enables us to restore specific objects or groups on that system if needed.</p>
----	--	--

48	Does it must also allow the organization to recall earlier versions of the environment.	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. We store a record of any accounts or entitlements associated with a user, including group memberships. This information is also stored within our audit database. Additionally, we can take snapshots of target systems account and group memberships which enables us to restore specific objects or groups on that system if needed.
49	Does it allow organizations to seamlessly move workflows, policies and configurations between dev, test and production environments.	Yes, 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.

50	When customizations are required, does solution provide support for common scripting languages including but not limited to such as JavaScript, Microsoft VBScript (Visual Basic Script), Python, etc.	Fischer has an innovative "configuration" vs. "coding" approach that reduces the solution administration, increases sustainability and simplifies compliance and audit processes. The Fischer solution was purpose built to eliminate the need for proprietary protocols and complex scripting tools that require specialized expertise. Fischer has addressed the common shortfall in most identity management systems by designing the configuration into the system so setup is performed in point and click UI. To allow for more powerful configuration of lifecycle management and target system provisioning, Fischer provides our Workflow and Connectivity studio, an intuitive tool for workflow development and deployment with the power of full export, transformation & load functionality ETL. The workflows are not proprietary, instead they are stored and deployed XML objects.
51	Does it include integration APIs that allow third-party systems to access data and system functions - entitlements, policies, access, roles, workflow, etc.	The solution has a published set of REST API's.
52	Does it provide an administrative interface to manage access/API keys.	Fischer has REST API / SOAP API and supports import via SOAP and export via REST. Modification of user data is available using REST. Fischer has a REST API Developer's Guide that lists the base URL and the Identity Objects exposed via REST services.

53	Does solution provide the ability to restrict what data elements are available to the third-party systems. API's should support message brokers such as JMS and RabbitMQ.	Third party service provides do not have access to data.
54	Describe how access controls and cryptographic techniques are used to protect sensitive data housed in the system. Include configurable system security policies in your response	<p>Data at rest: We encrypt with symmetric keys sensitive data at rest. Since our product is customizable and can treat different data, we also offer the option to encrypt parts of the processed data.</p> <p>Data in transit: Our product has different pieces that communicate with each other. Communication happens through web-services or through a replicated cache. The web-services calls are authenticated and signed. If any encrypted data is being sent over through a web-service, it is re-encrypted over the wire with previously shared asymmetric keys. If web-services calls are made over a non-secure network, we require that SSL is setup at the server level. The replicated cache uses JBoss Group technology to communicate. It is setup to use authentication and asymmetric encryption by default.</p> <p>Digital signatures: For sensitive applications, the user's entire session is protected via SSL, based on 1024-bit RSA or equivalent digital signatures.</p> <p>Key Management: Our product provides a built-in key management feature that allows key rotation for both symmetric keys and asymmetric keys. Our symmetric keys are used to encrypt data at rest and different keys are used for different data type. Our asymmetric keys are used for data in transit encryption. Keys are stored in a Java key-store on disk. In a highly available environment, keys are synchronized between instances using appropriate key exchange algorithm.</p> <p>Fischer Identity includes a robust set of configurable system security policies to ensure fine-grained security controls that restrict access to data and functions in the system. Users are presented with only the resources and profile attributes that they are authorized to select, view or modify, ensuring that the "principle of least privilege" is always enforced.</p>

55	Describe change management processes including documentation, workflow approvals, email notifications or other safeguards.	<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. Authorized users e.g. Administrators and Auditors can login into self-service to configure, run view and share the reports.</p>
56	Describe how log and audit information generated by the solution are transmitted and stored in such a fashion that they cannot be altered or deleted without being detected.	Fischer timestamps all logs and stores like data in multiple locations.

57	Does solution provide a mechanism for authentication of administrators, using two factors of authentication or other methods exceeding the strength of simple username and password.	Fischer provides Shibboleth/SAML and native DUO Support. Fischer provides multiple authentication methods to meet your demands for identity assurance, transaction integrity, and usability. Fischer Authenticator™, an intuitive multifactor authentication app establishes the level of trust you need before granting access to the Fischer ecosystem. Up to 5-factors of authentication may be used: Pattern Code, Fingerprint Scan, Pin Code, Geofencing, and Bluetooth Proximity. Fischer Authenticator™ also supports the "Two-Person Rule". The Two-Person Rule requires that two or more individuals simultaneously authorize and authenticate to obtain access, authorize an action, or other function. Fischer also supports Duo Multifactor authentication.
----	--	---

58	Access Policies	<p>Fischer can qualify / disqualify users with specific parts of their overall roles. 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.</p> <p>Once resources accounts, groups, roles, etc. are configured in the resource catalog, they are available for assignment, either through automated provisioning or by request. Owners and approvers can be configured and associated along with permissions and dependencies. These resources are then available for role and attribute-based provisioning and tied to the policy catalog. Access rights are assigned and managed though policies conditions configured in the zero coding UI. The result is a consolidated catalog of system resources and qualifications. Birthright access rights are assigned by relational conditions while requested or assigned access is managed independently and monitored through delegated administration. As part of the evolution of control the Fischer solution recognizes the need for "all boarding", which is powerful support to provide, remove and restore access in alignment with organizational security policy and the user requirements and productivity within that context.</p>
----	-----------------	--

59	Can all functions be processed through a centralized access policy enforcement component.	<p>Fischer can qualify / disqualify users with specific parts of their overall roles. 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.</p> <p>Once resources accounts, groups, roles, etc. are configured in the resource catalog, they are available for assignment, either through automated provisioning or by request. Owners and approvers can be configured and associated along with permissions and dependencies. These resources are then available for role and attribute-based provisioning and tied to the policy catalog. Access rights are assigned and managed though policies conditions configured in the zero coding UI. The result is a consolidated catalog of system resources and qualifications. Birthright access rights are assigned by relational conditions while requested or assigned access is managed independently and monitored through delegated administration. As part of the evolution of control the Fischer solution recognizes the need for "all boarding", which is powerful support to provide, remove and restore access in alignment with organizational security policy and the user requirements and productivity within that context.</p>
----	---	--

60	<p>Can your solution support multiple types of access policies, including: Assignment policies: Determine whether the assignment of an entitlement (like a role) is allowed by policy.</p> <p>Approval policy: Determine whether or not approvals are required before fulfillment, and if so, identify approvers.</p> <p>Detachment: Determine how an entitlement should be removed once the assignment policy no longer applies.</p> <p>Visibility: Determine who can see an entitlement for purposes of requesting access or other functions.</p>	<p>Assignment policies: Determine whether the assignment of an entitlement (like a role) is allowed by policy. Supported.</p> <p>Approval policy: Determine whether or not approvals are required before fulfillment, and if so, identify approvers. Supported.</p> <p>Detachment: Determine how an entitlement should be removed once the assignment policy no longer applies. Supported.</p> <p>Visibility: Determine who can see an entitlement for purposes of requesting access or other functions. Supported.</p>
61	<p>Does it support the following three types of access policy assignment methods: Rule-based access policy assignment: Access policies are defined using a set of conditional rules. Role-based access policy assignment: Access policies are defined using roles. Workflow-based access policy assignment: Access policies are defined through a series of approval workflows.</p>	<p>Yes, Rule-based access policy assignment, Role-based access policy assignment and Workflow-based access policy assignment are supported.</p> <p>The Fischer Solution is unique in how qualification for policy is configured and access granted. Conditions related to the user's attributes are evaluated through powerful evaluation engine to determine qualification. This can be based on Attribute or Role. In the Workflow Studio, even more powerful evaluation rules can be used including relationship and external sources.</p>

62	Does it support both static and dynamic policy definition. Static policies are based on an explicit or named value. Dynamic policies are based on an attribute or a dynamic field	Yes, Fischer supports support both static and dynamic policy definition.
63	Does it allow organizations to define both business and technical roles and allow business roles (as well as individual users) to be assigned to technical roles	<p>Fischer's role management supports a many-to-many model. Role are defined within the system which will drive what access a user will qualify for. They are not limited in the number of roles they can qualify for and roles can changed depending on the other roles a user is a part of. Example if a Staff member receives access to reset user's passwords but they are also a student, their access can be limited to only the population of users they should have access to. Thus they would not have the ability to reset faculty passwords.</p> <p>The administration portal allows you to have a complete view of what a user's roles are, who are members of a role, what account and entitlements the user has. Reports can be made available that allows you visibility into what roles have which entitlements.</p>

64	<p>Does role structure support a role model in which permissions are assigned to roles, users are assigned to roles and users inherit permissions based on their role assignment</p>	<p>Fischer's role management supports a many-to-many model. Role are defined within the system which will drive what access a user will qualify for. They are not limited in the number of roles they can qualify for and roles can changed depending on the other roles a user is a part of. Example if a Staff member receives access to reset user's passwords but they are also a student, their access can be limited to only the population of users they should have access to. Thus they would not have the ability to reset faculty passwords.</p> <p>The administration portal allows you to have a complete view of what a user's roles are, who are members of a role, what account and entitlements the user has. Reports can be made available that allows you visibility into what roles have which entitlements.</p>
----	--	--

65	Does it support a many-to-many model in which a user can have multiple roles and a role can have multiple users	<p>Fischer's role management supports a many-to-many model. Role are defined within the system which will drive what access a user will qualify for. They are not limited in the number of roles they can qualify for and roles can changed depending on the other roles a user is a part of. Example if a Staff member receives access to reset user's passwords but they are also a student, their access can be limited to only the population of users they should have access to. Thus they would not have the ability to reset faculty passwords.</p> <p>The administration portal allows you to have a complete view of what a user's roles are, who are members of a role, what account and entitlements the user has. Reports can be made available that allows you visibility into what roles have which entitlements.</p>
66	Does it support a hierarchical role model in which roles inherit permissions from other roles.	The solution supports nested policies and relationships for target systems allowing for flat and hierarchical role models.

67	<p>Describe if your solution include different views of role data, including: User role assignment: From a user object, view all role assignments Role membership view: From a role object, view all users assigned to the role Role entitlement view: From a role object, view all entitlements associated with the role Entitlement view: Discover all roles that include a specific entitlement</p>	<p>The administration portal allows you to have a complete view of what a user's roles are, who are members of a role, what account and entitlements the user has. Reports can be made available that allows you visibility into what roles have which entitlements.</p>
68	<p>Once a policy has been updated, does the solution must provide a mechanism to reapply roles and policy to users.</p>	<p>When a role changes, the solution will provision changes for all users that have that role.</p>
69	<p>Does it support both static (specific combination of roles) and dynamic (user not acting in 2 roles simultaneously) policy definitions for separation of duties.</p>	<p>Access policies are configured with Allow, Deny, Approval and Object security all based on attribute or role conditions. In addition, direct Separation of Duties are configured to limit toxic combinations and alert compliance monitors.</p>

70	Describe ability to handle separation of duty controls across multiple applications at a fine-grained level.	<p>Fischer is built to handle compliance through several different methods.</p> <p>First, Fischer allows you to define roles and create separation of duty rules. These rules can initiate notification and/or actionable items that a authorized user can determine if the violation is valid.</p> <p>Second, Fischer can be configured to handle certifications that allow your authorized users to verify user access, create exceptions or handle violations as part of the certification campaign. Certification allows your certifiers to review and determine if current access is valid and the system will display any anomalies such as excessive or missing access for a user.</p> <p>Finally, real-time monitoring can be implemented to catch any violations to access and take immediate action. This can initiate an approval processes, removal of access, or notification to appropriate users. If approvals are used, they can be used to remove access or retain access based on the approval flow outcome.</p>
71	Describe your solution's workflow approval process including but not limited to allowing business owners or delegated administrators to accept or reject the proposed change on an individual user basis, when a permission is changed or removed from a role.	<p>When a role changes, the solution will provision changes for all users that have that role. An approval process can be set up to allow business owners or delegated administrators to accept or reject the proposed change on an individual user basis</p>

72	Does solution include a graphical user interface for modeling and editing policy and role definitions.	Roles can be designed and modeled using the administrative user interface. This includes the ability to build conditions and rules from identity attributes to be used for role qualification. Rules and conditions can be modeled to show what users 'would' qualify based on the changes and then allow administrators to accept or reject those changes based on the results of their modeling.
73	Can administrators create, modify and delete policies and roles from the editing tool.	Yes, The administration portal allows you to have a complete view of what a user's roles are, who are members of a role, what account and entitlements the user has. Reports can be made available that allows you visibility into what roles have which entitlements. You can create, modify and delete policies and roles from the editing tool. This includes the ability to build conditions and rules from identity attributes to be used for role qualification. Rules and conditions can be modeled to show what users 'would' qualify based on the changes and then allow administrators to accept or reject those changes based on the results of their modeling.

74	Does solution include a graphical user interface that allows business owners to design and manage roles.	Roles can be designed and modeled using the administrative user interface. This includes the ability to build conditions and rules from identity attributes to be used for role qualification. Rules and conditions can be modeled to show what users 'would' qualify based on the changes and then allow administrators to accept or reject those changes based on the results of their modeling.
----	--	--

Table 5 – Identity Governance Part C

1	Does your solution support workflow processing and include a workflow engine.	Yes, Fischer's 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.
2	Does your solution provide email notifications that notify participants of status changes and work items. Must be able to customize email templates and be able to utilize different templates based upon workflow.	Notifications to the approvers, requester, beneficiary and administrators are all configurable with independent notify conditions and messages. Custom attributes can be required of approvers and approvers may request additional information, sending the request back to the requester or prior approvers for action. Of course approval history is fully maintained both for the individual requests and in the audit record. Configured approvals can be used in workflows by the Workflow and Connectivity Studio for automated and user initiated tasks.
3	If a workflow task is not completed within a given time period, can it send a reminder to the person assigned the workflow task.	Fischer Identity provides for powerful approval support. Serial, parallel, and hierarchical approval routing with escalations, response time out, reassignment, overrides, exception handling, and delegation all are supported.
4	If the reminder did not get the task finished within a given time period, is it able to redistribute the task to another approver.	Fischer Identity provides for powerful approval support. Serial, parallel, and hierarchical approval routing with escalations, response time out, reassignment, overrides, exception handling, and delegation all are supported.
5	Can it support workflows that need to climb a hierarchal chain of organizational approvals. This may continue to the highest level in the organization.	Yes, approval chains can be configured for specific systems before access is granted.

6	Does it allow an approver to select a delegate and delegate all or a subset of line items to the delegate. The delegation should also include an effective date (begin and end date). Must allow the assigned workflow task to be reassigned to another user.	Yes, Approval delegation is configurable and supported in the Self-Service application including managed availability.
7	Is it able to permit a subset of reviewers to approve (m of n) or all reviewers to approve (n of n).	Fischer Identity provides for powerful approval support. Serial, parallel, and hierarchical approval routing with escalations, response time out, reassignment, overrides, exception handling, and delegation all supported. Approvals can be attached to resources and entitlements, role policies, and individual profile attributes. Approvers are configured from the users identity users or external LDAP based on static or dynamic assignment of individuals, groups, resource ownership and or system ownership. Notifications to the approvers, requester, beneficiary and administrators are all configurable with independent notify conditions and messages. Custom attributes can be required of approvers and approvers may request additional information, sending the request back to the requester or prior approvers for action. Of course approval history is fully maintained both for the individual requests and in the audit record. Configured approvals can be used in workflows by the Workflow and Connectivity Studio for automated and user initiated tasks.
8	Does solution Allow an approver to reroute the workflow task back to the originator or a previous approver for additional input.	Approvers may reroute workflow tasks back to the originator or previous approvers for additional input or clarifying information.
9	Can solution be able to complete workflow tasks sequentially or simultaneously (serial or parallel).	Serial, parallel, and hierarchical approval routing with escalations, response time out, reassignment, overrides, exception handling, and delegation all supported. Conditional workflow processing as part of the workflow engine, where workflow steps can be dynamically determined by the outcome of other workflow step is configurable.
10	Does your support both static and dynamic approval routing, determined through a dynamic field lookup or named explicitly.	Serial, parallel, and hierarchical approval routing with escalations, response time out, reassignment, overrides, exception handling, and delegation all supported. Conditional workflow processing as part of the workflow engine, where workflow steps can be dynamically determined by the outcome of other workflow step is configurable.

11	Does your support conditional workflow processing where workflow steps are dynamically determined by the outcome of other workflow steps.	Yes, conditional workflow processing as part of the workflow engine, where workflow steps can be dynamically determined by the outcome of other workflow step is configurable.
12	Can the workflow engine able to invoke external processes and services using web services, APIs or local execution. Explain	Workflows orchestrate a logical sequence of steps to enable critical functions such as access approvals, access reviews and identity life cycle management. Workflows allow business stakeholders, application owners and other authorities to validate and approve proposed changes before they are applied to target applications. Workflows are able to accept return codes, process data and monitor the status of activity from the external application.
13	Can your solution manage the interaction between the workflow engine and the invoked application or service.	Workflows allow business stakeholders, application owners and other authorities to validate and approve proposed changes before they are applied to target applications.
14	Can your solution accept return codes, process data and monitor the status of activity from the external application. Explain	Workflows are able to accept return codes, process data and monitor the status of activity from the external application.
15	Does the interface allow approvers to view, track and manage all workflow tasks assigned to them from a single location.	The requester has a status view, approval authorities have a queue of pending requests and can view current work list items as well as a history of work list items assigned to the approver. Attachments and supporting data can be added to the request. Electronic signature capability for workflow approvals is customizable.
16	Does your solution include current work list items as well as a history of work list items assigned to the approver.	The requester has a status view, approval authorities have a queue of pending requests and can view current work list items as well as a history of work list items assigned to the approver.
17	Does your solution allow participants to attach files to the workflow; Does it allow for approvers to add an electronic signature to a workflow for business, legal, or regulatory purposes. Explain	Attachments and supporting data can be added to the request. Electronic signature capability for workflow approvals is customizable.
18	To help simplify workflow design, does it include a graphical workflow design and/or textual workflow design. Explain.	Our studio provides point and click, drag and drop usability to build complex workflows without compiling code. Visual tools, intuitive design and data mapping functionality, connectivity and schema discovery allow you to build complex workflows without the traditional coding or scripting required in other identity systems.

19	Does your solution include a set of normalized, predefined workflow templates that can be modified to meet unique organizational needs.	Standard.
20	Describe your solution's configurable policies for handling policy violations, including the following Ability to define alerts based on predefined criteria. Ability to trigger a notification if a violation is detected. Ability to trigger a workflow approval if a violation is detected. Ability to automatically adjust the user record according to policy. Ability to define the individuals who are able to respond to specific policy violations. Ability to flag high-risk entitlements, accounts, access, roles, etc. Ability to configure or define compensating controls that dictate that action to take if a risk score changes. Ability to flag out-of-compliance entitlements, accounts, access, roles, etc. Ability to review and certify the accuracy of data elements. Ability to review and assign or claim orphaned accounts. Ability to detect, review, and assign dormant accounts that have not been used for a specified period of time. Ability to analyze and compare access of users in a specified peer group and to detect users with excessive access or outliers whose access is different than their peer group.	<p>Fischer is built to handle compliance through several different methods.</p> <p>First, Fischer allows you to define roles and create separation of duty rules. These rules can initiate notification and/or actionable items that a authorized user can determine if the violation is valid.</p> <p>Second, Fischer can be configured to handle certifications that allow your authorized users to verify user access, create exceptions or handle violations as part of the certification campaign. Certification allows your certifiers to review and determine if current access is valid and the system will display any anomalies such as excessive or missing access for a user.</p> <p>Finally, real-time monitoring can be implemented to catch any violations to access and take immediate action. This can initiate an approval processes, removal of access, or notification to appropriate users. If approvals are used, they can be used to remove access or retain access based on the approval flow outcome.</p>
21	Does your solution support multiple methods for calculating a risk score, including:Ability to calculate risk based on a static risk score value that is assigned directly to an entitlement.Ability to calculate risk based on an algorithm that derives a risk score based on multiple factors.Ability to calculate risk based on the role, account or system to which a user is assigned.Ability to calculate risk based on a violation of a policy.	Fischer Identity is able to manage risk profiles through provisioning and authentication policies based upon an identity's attributes. Identities with riskier attributes, such as roles or titles, location, or other attributes giving access to higher security systems, may be forced into stronger authentication policies, including the use of two-factor authentication for only those users who qualify. This could also be based upon a cumulative set of attributes triggering such risk-based policies. Using this capability, the Fischer solution can monitor login activity and adjust the user profile by moving the user to a higher risk category and enforcing more stringent login standards for

		Captcha, MFA, TOTP, SecQA, etc. More advanced risk profiling capability is planned for future releases.
22	Can your solution allow organization to set audit controls that are used by audit scans to detect policy violations	Fischer logs all 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.
23	Is there flexibility to cover multiple control types, such as segregation of duties, profile integrity and rogue accounts.	Fischer logs all 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.
24	Is there ability to displaying a risk score associated with users' access, whether that is a static risk score or a dynamic risk score derived from analytics.	Fischer logs all 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.

25	Describe the User Interface provided relating to user-friendly console or dashboard that allows administrators to manage controls, visualize performance and monitor violation handling.	Fischer provides an accessible audit store that contains information about all actions and activities that occur within the platform. 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. The native reporting interface contains approximately 100 canned reports and the ability to build custom reports covering all aspects of the product in a multitude of views. Log files are also available and updated in real-time. Fischer provides multiple levels of logs info, debug, all, including a plethora of data.
26	Does the user interface have the ability to maintain a historical snapshot of identity data and report on a user's access at any time.	Fischer has a centralized identity directory/repository that supports multiple concurrent identity-related roles and affiliations and stores both current and historical data.
27	Does the User Interface provide the ability to log all events processed through the solution infrastructure in the audit repository, including ILM, fulfillment, workflow, entitlement management, access request and access certification events.	Fischer provides an accessible audit store that contains information about all actions and activities that occur within the platform. 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. The native reporting interface contains approximately 100 canned reports and the ability to build custom reports covering all aspects of the product in a multitude of views. Log files are also available and updated in real-time. Fischer provides multiple levels of logs info, debug, all, including a plethora of data

28	<p>Describe how the solution address Access Certification in the following areas: Flexible scheduling utility that allows organizations to define the intervals in which access certifications will be run. Allows for annual, semiannual, quarterly, weekly and daily intervals. Allows for access certifications to be run continuously for high-risk or closely monitored users or entitlements Supporting a single certification that is run outside of the normal access certification schedule. Integrate with access request and access certification process with data such as risk score, anomalies, outliers, dormant accounts and so on.</p>	<p>You can review access for users in the context of access policies, accounts and entitlements. You can "allow", "remediate", or "remove" access during the review process. 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 Fischer compliance system supports powerful configuration beginning with the definition of Chain of Trust made up of certifiers, or users selected statically specific user or dynamically logical expression. Certifiers can be assigned to groups of users for the purposes of attestation reviews. The Chain of Trust is assigned to Compliance jobs where policies, resources accounts and/or entitlements, and systems are configured for assessment and/or review by the Chain of Trust and optionally parallel technical review. Certifiers can "allow", "remediate", or "remove" access during the review process. Compliance assessments can be executed on a scheduled basis to find and report all access control policy violations and present audit controllers with remediation options as well as override options, including access certification.</p>
----	---	--

29	<p>Describe key functionalities of the dashboard taking into account the following: Can filters be global (refining scope for the entire dashboard) or local (refining scope for a specific chart, metric or view). Does it include a comprehensive set of common KPIs that are built into the dashboard. Does it allow organizations to customize default KPIs and save the changes. Does it include the ability to define unique KPIs and include them in the dashboard. Does it provide the ability to set thresholds on KPIs that provide visualization cues or notifications when specific conditions have been met. Does it provide visual tools that display a heat map, speedometer or other visual aid to alert users to threshold status. Does it support advanced visualization functions, including geographic maps, tag clouds, scatterplots and bubble charts. Does solution have ability for users to identify things such as ability to add commentary or annotation to specific components of a dashboard.</p>	<p>Fischer Identity has an Operational Dashboard that organizes and presents information in a way that is easy to read, understand, and analyze. It enables administrators to view current and historic statistical information about the operation of various components of the Identity and Provisioning Servers, as well as Global Identity Gateways.</p> <p>The Operational Dashboard uses the Flex application framework. The latest version of the Flash Player plug-in is required to view the Operational Dashboard.</p> <p>The Operational Dashboard data collection process consists of a thread per server that manages a FIFO queue. Messages are posted to the queue as and when events occur by different components of the IdM Suite. For example, when a user logs in, a corresponding message is posted to the data collector. The queue is flushed periodically by the post-processor thread, which consolidates the messages before being written out to the Dashboard database.</p> <p>Operational Dashboard Overview</p> <p>The Operational Dashboard enables administrators to monitor the IdM Suite 24/7. An administrator who qualifies for the Master Administration or Monitor Administration security policy will see the Dashboard tab after logging in to Identity.</p> <p>The Operational Dashboard UI has five sub tabs, which represent the Summary view and the detailed views.</p>
----	---	--

30	<p>Describe the ability to run reports on the following: Usage and effectiveness of roles over time. User activity, login, and usage data. Access certification: Full certification that includes a complete set of user or entitlement data (as defined by the scope). Delta certification that includes only the user or entitlement data that has changed since the last certification. Have the ability to customize default reports and save the changes. Provide ability to create custom user defined reports. Users should be able to define the scope of the returned data in the report to meet their needs. Scheduling a report to run at a particular time or after an event has been executed. Provide the ability to export report results to a CSV, PDF or HTML file format.</p>	<p>Fischer provides an accessible audit store that contains information about all actions and activities that occur within the platform. 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. The native reporting interface contains approximately 100 canned reports and the ability to build custom reports covering all aspects of the product in a multitude of views. Log files are also available and updated in real-time. Fischer provides multiple levels of logs info, debug, all, including a plethora of data. Sample reports, logs and audit trails are available under NDA.</p>
31	<p>Does the solution have predefined set of reports for common functions, including user life cycle, access certification, access request, passwords, roles and so on.</p>	<p>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. The access control model allows for delegated access in the self-service application for authorized users to build, run, share and download the reports.</p>

32	<p>Our user lifecycle processes are driven from data in multiple source systems. Users can transition between multiple statuses in varying combinations within those source systems (e.g., "student", "former student", "employee", "student employee", "faculty", "staff"), each of which has associated access rules, some overlapping or potentially conflicting. As users transition across these statuses the IGA system should be able to appropriately manage their access to systems, all tied to the same campus primary campus identity.</p>	<p>Fischer would address this scenario by using role based access control to govern what user accounts and access the student has associated with them. When the student enrolls that will trigger certain access like NetID to be provisioned for the user, access to their record in Banner, a Google e-mail address, wireless and lab computer access.</p> <p>Once the student is hired they would now qualify for access as both a student and an employee. Fischer would retain all their student access while provisioning them with their new access associated with their employee status.</p> <p>When the student graduates but is hired as an employee, they would now lose all access related to being a student while most likely gaining access as an alumni or un-enrolled user. They would retain their employee access.</p> <p>Using this methodology allows you to maintain the user of one NetID instead of using multiple. Fischer Can consume information from multiple sources of authority, allowing you to combine user data into a single record. This will eliminate the need to provisioning multiple accounts for the same user because they have different affiliations.</p>
----	--	--

33	<p>Related to scenario 1 describe how a user lifecycle might play out. Please describe how we can implement these flows in your system, and the best practices to manage and audit these kinds of user access.</p>	<p>Fischer would address this scenario by using role based access control to govern what user accounts and access the student has associated with them. When the student enrolls that will trigger certain access like NetID to be provisioned for the user, access to their record in Banner, a Google e-mail address, wireless and lab computer access.</p> <p>Once the student is hired they would now qualify for access as both a student and an employee. Fischer would retain all their student access while provisioning them with their new access associated with their employee status.</p> <p>When the student graduates but is hired as an employee, they would now loose all access related to being a student while most likely gaining access as an alumni or un-enrolled user. They would retain their employee access.</p> <p>Using this methodology allows you to maintain the user of one NetID instead of using multiple. Fischer Can consume information from multiple sources of authority, allowing you to combine user data into a single record. This will eliminate the need to provisioning multiple accounts for the same user because they have different affiliations.</p>
----	--	---

34	<p>Related to scenario 1 student enrolls at the university, as indicated by data in the campus student system. In response the IGA system creates [or updates an existing] a campus identity (e.g., NetID, loginID, UserID). As a current student, the user is provisioned access to the student system (e.g., to see grades/transcript), the campus email system email, the wireless network, and lab computers.</p>	<p>Fischer would address this scenario by using role based access control to govern what user accounts and access the student has associated with them. When the student enrolls that will trigger certain access like NetID to be provisioned for the user, access to their record in Banner, a Google e-mail address, wireless and lab computer access.</p> <p>Once the student is hired they would now qualify for access as both a student and an employee. Fischer would retain all their student access while provisioning them with their new access associated with their employee status.</p> <p>When the student graduates but is hired as an employee, they would now loose all access related to being a student while most likely gaining access as an alumni or un-enrolled user. They would retain their employee access.</p> <p>Using this methodology allows you to maintain the user of one NetID instead of using multiple. Fischer Can consume information from multiple sources of authority, allowing you to combine user data into a single record. This will eliminate the need to provisioning multiple accounts for the same user because they have different affiliations.</p>
----	---	---

35	<p>Related to scenario 1 - the student is later hired as a Student Employee (reflected by data in the systemwide HR system). The student maintains all access noted above, but their identity record is updated to include their employment information, and as a current student employee they are also provisioned access to the campus training and data storage solutions.</p>	<p>Fischer would address this scenario by using role based access control to govern what user accounts and access the student has associated with them. When the student enrolls that will trigger certain access like NetID to be provisioned for the user, access to their record in Banner, a Google e-mail address, wireless and lab computer access.</p> <p>Once the student is hired they would now qualify for access as both a student and an employee. Fischer would retain all their student access while provisioning them with their new access associated with their employee status.</p> <p>When the student graduates but is hired as an employee, they would now lose all access related to being a student while most likely gaining access as an alumni or un-enrolled user. They would retain their employee access.</p> <p>Using this methodology allows you to maintain the user of one NetID instead of using multiple. Fischer Can consume information from multiple sources of authority, allowing you to combine user data into a single record. This will eliminate the need to provisioning multiple accounts for the same user because they have different affiliations.</p>
----	--	--

36	<p>Related to scenario 1 the student then graduates and is terminated as an student employee (reflected by data in the student system). As a former student they immediately lose access to the lab computers, they maintain access to their email and the wireless system for 90 days, and they maintain login access to the student system indefinitely. As a former employee they immediately lose access to the training and data storage solutions, but their data and profiles are maintained in an inaccessible state.</p>	<p>Fischer would address this scenario by using role based access control to govern what user accounts and access the student has associated with them. When the student enrolls that will trigger certain access like NetID to be provisioned for the user, access to their record in Banner, a Google e-mail address, wireless and lab computer access.</p> <p>Once the student is hired they would now qualify for access as both a student and an employee. Fischer would retain all their student access while provisioning them with their new access associated with their employee status.</p> <p>When the student graduates but is hired as an employee, they would now loose all access related to being a student while most likely gaining access as an alumni or un-enrolled user. They would retain their employee access.</p> <p>Using this methodology allows you to maintain the user of one NetID instead of using multiple. Fischer Can consume information from multiple sources of authority, allowing you to combine user data into a single record. This will eliminate the need to provisioning multiple accounts for the same user because they have different affiliations.</p>
----	---	---

37	<p>Related to scenario 1 - Shortly thereafter the former student is rehired as a staff employee. The staff employee regains (or has the pending termination of access halted) access to their previous email, wireless, training and data storage services.</p>	<p>Fischer would address this scenario by using role based access control to govern what user accounts and access the student has associated with them. When the student enrolls that will trigger certain access like NetID to be provisioned for the user, access to their record in Banner, a Google e-mail address, wireless and lab computer access.</p> <p>Once the student is hired they would now qualify for access as both a student and an employee. Fischer would retain all their student access while provisioning them with their new access associated with their employee status.</p> <p>When the student graduates but is hired as an employee, they would now lose all access related to being a student while most likely gaining access as an alumni or un-enrolled user. They would retain their employee access.</p> <p>Using this methodology allows you to maintain the user of one NetID instead of using multiple. Fischer Can consume information from multiple sources of authority, allowing you to combine user data into a single record. This will eliminate the need to provisioning multiple accounts for the same user because they have different affiliations.</p>
38	<p>University identity systems receive user information from multiple authoritative sources (student information systems, HRIS, University Extension programs, etc.). The population cannot be assumed to have a common, immutable attribute matching attribute (such as SSN). Please describe how your solution addresses this matching issue to minimize the creation of duplicate accounts.</p>	<p>Using our powerful identity matching, if the same identity came from separate sources of authority, the matching system would pause the provisioning activity until the match could be resolved. Then independent processing of the new authoritative identity record would continue. Additionally, the Fischer Identity solution isolates the attribute policy mapping independent from the managed system connectors so that we can simultaneously pull identity information from multiple authoritative sources. We call this process staging with delta processing. The sources can be of multiple technologies and we export adds, changes and deletes from the SoAs and consolidate them into identity events.</p>

39	<p>It is common for users within a university identity system to exist in multiple authoritative source systems. For example, a student-employee's identity record will contain information from both the HR and student systems. How does your solution address the circumstance where the authoritative sources are not in agreement on an attribute? Please describe how your solution escalates or resolves these conflicts.</p>	<p>Using our powerful identity matching, if the same identity came from separate sources of authority, the matching system would pause the provisioning activity until the match could be resolved. Then independent processing of the new authoritative identity record would continue. Additionally, the Fischer Identity solution isolates the attribute policy mapping independent from the managed system connectors so that we can simultaneously pull identity information from multiple authoritative sources. We call this process staging with delta processing. The sources can be of multiple technologies and we export adds, changes and deletes from the SoAs and consolidate them into identity events.</p>
40	<p>In the course of business, there will be cases where a single individual ends up with multiple identities (e.g. multiple NetIDs for the same individual) due to a match failure. Please describe how your solution addresses the consolidation of these into a single identity record including reconciling any differences in attributes, updating downstream services, and any audit capabilities.</p>	<p>During user load processing Fischer can perform "lookups" into the target system or other systems to verify if the record already exists. Records that already exist can be ignored or merged with the existing records based on a set of rules that are defined during the solution design and loading phase.</p>
41	<p>There will also be cases where a two different individuals are incorrectly identified as being the same person, and only one identity is created. Please describe how your solution addresses separating these identities into two separate identities including updating permissions, access rights and accounts in downstream services, also including any audit capabilities.</p>	<p>The Fischer solution is usually configured to assign a persistent unique identifier. Depending on the configuration requirements, existing unique identifiers, and source of authority processing, the unique ID may be configured to align with one or more of these source systems. Internally, Fischer maintains it's own GUID to ensure that changes to unique ID or other need for persistent record identification is maintained.</p> <p>Fischer can create this unique identifier in any format you require using Fischer's data mapper. The data mapper is where the business logic is scripted and data is validate and manipulated.</p>
42	<p>We have a number of applications whose user profiles, user authentication and user access/roles should be derived from information in the IGA system. Describe how your solution discovers and onboards such applications, including but not limited to:</p>	<p>Using Fischer's Studio which has a powerful Extraction, Transformation, Load ETL Engine which enables us to extract users and roles from a connected application. Once extracted, the output can be reviewed to determine which roles are 'in-use'. After the role list is created, the roles can be imported into Fischer's Resource Repository and then</p>

		associated with existing IGA Roles and/or new IGA roles can be created.
43	Configuring the IGA and application to allow the IGA to provision and manage users, user profiles, role assignments, etc. based on the existing data and roles in the IGA.	Using Fischer's Studio which has a powerful Extraction, Transformation, Load ETL Engine which enables us to extract users and roles from a connected application. Once extracted, the output can be reviewed to determine which roles are 'in-use'. After the role list is created, the roles can be imported into Fischer's Resource Repository and then associated with existing IGA Roles and/or new IGA roles can be created.
44	Detecting existing users and roles in an application, and mapping them to existing users and roles in the IGA system.	Fischer's connectors have real time schema detection, so once the connected system is configured, you can refresh the connector and it will pull back all of the attributes from the system. Once a connector is in place, you can build out the workflow and map the attributes per your business requirements.
45	Identifying and potentially modifying users or permissions that exist in the application that differ from those defined/approved in the IGA.	Fischer Connectors are bidirectional for the purpose of reconciliation and attestation. Fischer can utilize our ETL engine to create processes for reconciliation against any target that Fischer is managing. In scenarios where there are multiple SoAs, The client determines which SoA source is preferred for a given attribute and a workflow is created. If there is a conflict, the attribute from the preferred SoA is used.
46	Describe your recommended best practices for what aspects of user profile, account and role management are managed within an application vs. within your IGA system. E.g., should (or when should) high level and granular roles be managed locally in the application vs. managed in the IGA?	Ideally, all roles should be managed though the IGA. If not, Admin provisioning should be used to at least track the roles in the IGA system.
47	How does your solution support cases where some roles and profile elements are by different source systems; e.g., being managed locally within an app vs being provisioned from the IGA system vs being communicated as part of an authentication process (e.g., entitlements or grants included in a CAS/SAML/OAuth claim)?	The Fischer solution leverages its ETL engine in order to do reconciliation of data between sources of truth and other targets systems. This can be done in real-time during the processing of the record from the source of truth, or as a secondary process to reconcile the data during a scheduled process. You are capable of reconciliation not only from the source of truth, but any target system that Fischer is able to manage.

48	In the scenario where a staff member's access needs to be revoked immediately across multiple systems (including high privileged access). Describe how we can use your solution to centralize and simplify the de-provisioning of access. Address these kinds of scenarios	Access can be immediately revoked within the Identity Administration Portal with a single button click. Alternatively, we can detect specific attribute changes in a source of authority that would indicate a termination or termination with cause, that change would them remove the user from all access policies and immediate revoke all account access.
49	Access revoked to a subset of systems	Fischers deprovisioning policies allow for deletion, disabling or suspension of accounts. Placement policy can define inactive account location as well as define account retention policies. Fischer can qualify / disqualify users with specific parts of their overall roles. 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 is typically controlled by affiliations and roles. Fischer can not only handle multiple Sources of Record but also multiple affiliations.
50	Revocation of privileged access only	Fischer Identity comes out-of-the-box with a highly privileged access management module which can require administrative users to check-out privileged accounts, such as administrator, root, fire call, or DBA accounts for a limited period of time with full auditing of who owned and used a specific account at a specific point in time. This allows for administrators to only use privileged accounts when they need them rather than elevating privileges of their own identity within the organization via member of access to privileged groups such as Domain Admins, etc.
51	Temporary revocation of access (e.g., for a set period of time)	Fischer supports both "Account-EndDate" and "Account-StartDate" options, or what we call a future dated transactions that will automatically provision or de-provision access on the set date. This date can be set at initial provisioning time and can be extended or decreased throughout the life-cycle of the identity. You can revoke access at a set time and grant access to start again at a future date.

52	Ability to reverse revoked access in full, incrementally or to review and selectively reverse revoked access.	The Fischer compliance system supports powerful configuration beginning with the definition of Chain of Trust made up of certifiers, or users selected statically specific user or dynamically logical expression. Certifiers can be assigned to groups of users for the purposes of attestation reviews. The Chain of Trust is assigned to Compliance jobs where policies, resources accounts and/or entitlements, and systems are configured for assessment and/or review by the Chain of Trust and optionally parallel technical review. Certifiers can "allow", "remediate", or "remove" access during the review process. Compliance assessments can be executed on a scheduled basis to find and report all access control policy violations and present audit controllers with remediation options as well as override options, including access certification.
53	Similarly, there are many cases where access is automatically deprovisioned (see SCENARIO #1 for some examples). Describe how we can use your solution to support extensions of access or selective re-activation of access in cases where the extension is deemed warranted.	Fischer supports disabling identities or deleting them. The typical scenario is to disable for an extended period of time, then delete. Each system disables accounts differently. Depending on the system, Fischer would take the appropriate syntactically correct actions.
54	For example, an employee has separated, but an exception is granted to extend services to the employee to services for some (user defined) amount of time.	Fischer supports both "Account-EndDate" and "Account-StartDate" options, or what we call a future dated transactions that will automatically provision or de-provision access on the set date. This date can be set at initial provisioning time and can be extended or decreased throughout the life-cycle of the identity.
55	We have a variety of groups (i.e. Help Desk), administrative groups, and departmental admins who assist users that have different levels of access requirements for visibility to key identity information. Provide insight into best practices within your solution to address providing identity information to a variety of groups with varying levels of access.	Fischer ships with default Help Desk and Delegated Administrator roles. Additional help desk roles can be created using the default roles. Each help desk role can have a different features assigned. In addition to having different features for different help desk roles, you can control which users a specific help desk person can work on. For example, a student help desk person can be restricted to only working with 'students' or some subset of a student group while an employee help desk person can work with anyone in the directory.

56	Also describe how your solution supports and tracks changes made to user identity data.	Fischer's workflows can be designed in multiple ways to fit the customer's specific architectural and business requirements with both "real time" push and batch processing pull capabilities depending on system requirements. Triggers and SPML BEIS messages are supported for real-time event detection. In batch processing, Fischer automatically records the state of the export and can perform subsequent "delta" exports where only changed records are processed. Data synchronization processes are managed as Workflows built with the Fischer Studio. When changes are detected, either by push or pull, the process will determine what has changed added/modified/deleted and pass that change type to downstream process workflows and the provisioning engine. Workflows can be tied together and success and failure workflow processing initiated as the need dictates. When multiple sources of record are required to build a complete view of the identity's access requirements, Fischer architecture supports a "staging" process where changes are recognized
57	In some cases different administrative entities control management and creation of different source identities, or provisioning to downstream systems. How does your product support multiple administrative entities managing different aspects of user identities and user access?	Fischer provides a native security model empowering our customers to define a security hierarchy within the IAM application. Users and associated authorizations can be defined in a granular fashion. Attribute based access control is available to qualify users for delegated administration or approval authorizations based on particular attributes. Role based Access Control is also available. Each group is provided a set of permissions pertaining to what level of action they can take against the identity or identities they are authorized to administrate. This functionality extends across the entire product from administration to self-service interfaces. The information displayed to the user from their identity profile and what data fields they are allowed to modify is configurable from the Administration Console. Most institutions do not want users manipulating data such as Last Name on their own as that could have downstream effects on login ID's and email addresses.

58	<p>In some cases employees must be provisioned multiple accounts with separate passwords/credentials for use in different circumstances. E.g., Employees associated with both a Campus and Health Center at the same location may require one account that is used for HIPAA compliant purposes or elevated access purposes and another for non-sensitive purposes. How does your system support the intentional creation of multiple accounts (potentially with different permissions) for the same individual? And how can these separate accounts be managed by different administrative units (e.g., "Health IT" vs. "Campus IT")?</p>	<p>Fischer has a centralized identity directory/repository that supports multiple concurrent identity-related roles and affiliations and stores both current and historical data.</p>
59	<p>Many campuses support guests/external users - users needing access that do not exist in any formal campus source system.</p>	<p>Fischer Identity supports Self Registration for users, such as guest accounts. This allows the user to fill out pre-determined information to initiate the account creation process. The process can include approvals. The user will be created and credentials will be given.</p>
60	<p>How does your product support the creation of these categories of users both for creation of individual accounts (e.g., a contractor needing access, but not existing in any source system) and creation of accounts through ad-hoc data loads (e.g., individuals coming to campus to attend a multi-day seminar)? What is the workflow or process for supporting this kind of onboarding scenario? How does your product support delivery of these accounts to the guest users?</p>	<p>Fischer provides a self-registration feature for identities that do not exist in the SoA. Authorized users have the ability to create new identities directly within the Fischer product. This allows the user to fill out pre-determined information to initiate the account creation process. The process can include approvals. The user will be created and credentials will be given.</p> <p>Workflow can be written to automate the creation of the accounts. Using Fischer Account Claim user can claim and activate their account with a random one-time use authorization code and/or by validation of pre-populated information from a source of record. The claim information can be sent to the users during Source of Authority processing and their account credentials sent at that time or revealed during account claim. The Accounts can be set with either or both "Account-EndDate" and "Account-StartDate" options, or what we call a future dated transactions that will automatically provision or de-provision access on the set date. This date can be set at initial provisioning time and can be extended or decreased throughout the life-cycle of the identity.</p>

61	<p>In some cases, "guest accounts" are created in anticipation of the user having a future affiliation identified in a source system. E.g., an "incoming employee" might be assigned a guest account in anticipation of - but also in advance of - them being hired as an employee in the HR system. How does your system support incorporating these users into the overall user lifecycle process (Scenario #1) and user matching process (Scenario #2)?</p>	<p>This is standard functionality for Fischer. Multiple concurrent constituency types are supported via Identity Lifecycle Management ILM processes, including, faculty, staff, student, contractor, affiliate, applicant, alumni, and other user-defined constituency types, or roles out-of-the-box.</p>
62	<p>Frequently these users missing some of the typical matching data (e.g., SSNs, DoBs), but where matching between the guest and campus systems may be required. What capabilities or best practices exist in your system to support creation of users these users using custom matching logic, and to handle less precise user matches between source systems?</p>	<p>Using our powerful identity matching, if the same identity came from separate sources of authority, the matching system would pause the provisioning activity until the match could be resolved. Then independent processing of the new authoritative identity record would continue. Additionally, the Fischer Identity solution isolates the attribute policy mapping independent from the managed system connectors so that we can simultaneously pull identity information from multiple authoritative sources. We call this process staging with delta processing. The sources can be of multiple technologies and we export adds, changes and deletes from the SoAs and consolidate them into identity events.</p>
63	<p>For many systems, users must specifically request access, and that access must be approved and tracked on a per-request basis. In addition, some requests should be fulfilled (access granted) in a manner where the access is essentially conditional on some other information.</p>	<p>Fischer Self-Service Access Request feature enables users to request access or attribute changes and initiate the approval process, if required, through an intuitive, responsive web UI application for desktop, tablet, and mobile devices. Users are presented with only the resources and profile attributes that they are authorized to select, view or modify, ensuring that the "principle of least privilege" is always enforced. All events are fully audited, from request to approval. Authorized users may also request access on behalf of other users, make changes to existing access and remove access or even create users who don't appear in the sources of authority, such as contractors or vendors.</p>
64	<p>How does your product support access request and tracking workflows?</p>	<p>Access request status, workflow steps and approvers are be visible to the requester, the recipient, approvers and observers if applicable as configured by organizational policy. Access requests that have been submitted for approval, but not yet processed, can be canceled or modified. Requests can be submitted using pre-defined workflows.</p>

65	What kinds of conditions can your application support for maintaining or deprovisioning access?	Fischer supports disabling identities or deleting them. The typical scenario is to disable for an extended period of time, then delete. Each system disables accounts differently. Depending on the system, Fischer would take the appropriate syntactically correct actions.
66	Access granted for a specific time period	Fischer supports both "Account-EndDate" and "Account-StartDate" options, or what we call a future dated transactions that will automatically provision or de-provision access on the set date. This date can be set at initial provisioning time and can be extended or decreased throughout the life-cycle of the identity.
67	Access granted contingent on the user being a current employee or student	<p>Fischer would address this scenario by using role based access control to govern what user accounts and access the student has associated with them. When the student enrolls that will trigger certain access like NetID to be provisioned for the user, access to their record in Banner, a Google e-mail address, wireless and lab computer access.</p> <p>Once the student is hired they would now qualify for access as both a student and an employee. Fischer would retain all their student access while provisioning them with their new access associated with their employee status.</p> <p>When the student graduates but is hired as an employee, they would now lose all access related to being a student while most likely gaining access as a job title department change alumni or un-enrolled user. They would retain their employee access.</p> <p>Using this methodology allows you to maintain the user of one NetID instead of using multiple. Fischer can consume information from multiple sources of authority, allowing you to combine user data into a single record. This will eliminate the need to provisioning multiple accounts for the same user because they have different affiliations.</p>
68	Access review automatically prompted if the user's department, job title or other status information changes	Department, job title, or other status change can be configured to automatically trigger a workflow. The workflow can send notification to the users. The audit database stores action codes pertaining to events that occur within the system. These events can be monitored in real-time and flagged, reported on, or a workflow can be initiated to perform a task if desired / required.

69	Other capabilities or alternate approaches your application supports to address this kind of use case	Department, job title, or other status change can be configured to automatically trigger a workflow. The workflow can send notification to the users. The audit database stores action codes pertaining to events that occur within the system. These events can be monitored in real-time and flagged, reported on, or a workflow can be initiated to perform a task if desired / required.
70	Describe how your solution will address each of the following during an audit:	Fischer has a centralized identity directory/repository that supports multiple concurrent identity-related roles and affiliations and stores both current and historical data.
71	In preparation for the audit, how does your solution provide current and historical information on systems/applications and users ?	Fischer logs all 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.
72	How is historical information displayed on the UI?	Historical information is displayed in the UI in table format in the form of reports.
73	The auditor requires you to produce a report for history of access associated with a specific user.	<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. Authorized users e.g. Administrators and Auditors can login into self-service to configure, run view and share the reports.</p>

74	How would a Security Analyst be able to supply a report to their manager and an auditor?	<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. Authorized users e.g. Administrators and Auditors can login into self-service to configure, run view and share the reports.</p>
75	Does your product provide default dash boards?	<p>Fischer Identity has an Operational Dashboard that organizes and presents information in a way that is easy to read, understand, and analyze. It enables administrators to view current and historic statistical information about the operation of various components of the Identity and Provisioning Servers, as well as Global Identity Gateways.</p> <p>The Operational Dashboard uses the Flex application framework. The latest version of the Flash Player plug-in is required to view the Operational Dashboard.</p> <p>The Operational Dashboard data collection process consists of a thread per server that manages a FIFO queue. Messages are posted to the queue as and when events occur by different components of the IdM Suite. For example, when a user logs in, a corresponding message is posted to the data collector. The queue is flushed periodically by the post-processor thread, which consolidates the messages before being written out to the Dashboard database.</p> <p>Operational Dashboard Overview</p> <p>The Operational Dashboard enables administrators to monitor the IdM Suite 24/7. An administrator who qualifies for the Master Administration or Monitor Administration security policy will see the Dashboard tab after logging in to Identity.</p> <p>The Operational Dashboard UI has five sub tabs, which represent the Summary view and the detailed views.</p> <p>Summary View</p>

		<p>The Operational Dashboard's Summary tab displays the high-level Summary view of activities in the Identity and Provisioning Servers. The Summary view also has an Alert section that displays information on failed activities/server and Global Identity Gateway GIG status information as and when they happen. Details such as login failure, workflow failure, password reset failure, server or GIG down event, etc., display in this section. The Servers and GIGs section of the Summary view page provides information on the status, version, and JVM details memory, threads, and uptime.</p> <p>Detailed View</p> <p>Detailed monitoring information displays in the Provisioning, Self-Service, and Performance sub tabs. An administrator can monitor this information:</p> <ul style="list-style-type: none">Server status - Identity and Provisioning Server status.GIG - activities, status, and load.Database Connection Pool - for Identity and Provisioning Servers.Server performance - load and cache utilization.User activities.User request activities.Password reset activities.Approval activities.Workflow activities.Provisioning event activities.Resource allocation activities.Policy based provisioning activities.Compliance and recertification. <p>The Operational Dashboard provides detailed statistical information enabling administrators to determine what was happening at a particular point in time. This helps identify performance type issues or problems that are hard to recreate, besides giving information on the overall usage of the IdM Suite e.g., number of workflows that ran per server/organization, number of password resets, etc.. It also provides near real time data for visibility into what is happening now, and problem determination.</p> <p>The Operational Dashboard provides the following views with different date-time ranges:</p>
--	--	--

		<p>AV active view - The count for the last six hours.</p> <p>1D day view - The hourly count for the day.</p> <p>1W week view - The daily count for the week.</p> <p>1M month view - The daily count for the month.</p> <p>Range view - The count for the range selected.</p>
76	What is the retention period for historical information, and is this configurable?	The default retention periods is 365 days. The supported values are 1 to 10,000 days.
77	How is the full life cycle of access for an individual shown and reported?	The administration portal allows you to have a complete view of what a user's roles are, who are members of a role, what account and entitlements the user has. Reports can be made available that allows you visibility into what roles have which entitlements.
78	What functionality does the systems have to audit access and application life cycle management?	All activity and user account access is fully audited with attribute level support.

79	<p>How does your system detect when new accounts are added to the access management system, or when non-approved account changes are made to external systems, and how are these changes notified, reviewed, audited, etc.?</p>	<p>Fischer will detect changes adds/modifies/terminations in the source of authority by way of a scheduled workflow. This workflow can run on an iterative basis, defined by you. typically this is a once every hour event or some customers choose once per day. Once the event is received by Fischer we automate the action required based on the source event. For example if the user's last name changed and we need to rebuild usernames and modify the existing usernames for the user across multiple systems. The Fischer solution is usually configured to assign a persistent unique identifier. Depending on the configuration requirements, existing unique identifiers, and source of authority processing, the unique ID may be configured to align with one or more of these source systems. Internally, Fischer maintains it's own GUID to ensure that changes to unique ID or other need for persistent record identification is maintained. Fischer supports over 40 out of the box attributes. You can store as little or as much information as you'd like within our registry. Customer's typically display person bio data as well as affiliation data, location information, etc. Again, our registry is fluid and available to store whatever you need or want to store. From a downstream account perspective, Fischer stores the account username and the account id the ID will change per system and is the unique identifier we use to properly identify an account for password reset and audit purposes. We also store entitlement permission information such as group memberships within active directory, a database permission, etc.</p>
80	<p>We have legacy systems where access cannot be managed via a new solution, how does your solution address this situation to provide a full picture of someone's access?</p>	<p>Administrative Provisioning would create an account record in Fischer to log that an accounts exists in a given system that we do not have connectivity to for tracking.</p>



Table 6 - Fischer response to UC clarifications

- 1) What is the preferred (by a specific vendor) Access Management suite (Okta, etc) for your product?

Fischer's product abstracts authentication to enable our customers to make their preferred choice as it relates to Access Management. Overall, Fischer supports all standard protocols (OIDC, SAML 2, CAS, ADFS) in an effort to provide our customers options. Fischer provides a native, cloud-based Access Management solution, however we can also integrate with Okta, Ping, Quick Launch, Shibboleth, etc.

- 2) Please describe your integration process of your product with Azure and O/365 and are there any specific requirements or integration points that have been an issue for customers in the past?

Fischer communicates with Azure and O/365 using PowerShell. All connectors built in Fischer use the preferred method for communication such as available APIs, JDBC connection, LDAP, etc.

- 3) Does your product handle "just in time provisioning" scenarios? If so how does it handle this type of provisioning?

Note: Just-in-Time Provisioning is a method of automating user account creation for applications. It uses the SAML (Security Assertion Markup Language) protocol to pass information from the identity provider to web applications. So, when a new user tries to log in to an authorized app for the first time, they trigger the flow of information from the identity provider to the app that's needed to create their account.

Fischer's IdP will send the necessary attributes to a target Service Provider allowing the Service Provider the ability to create the user.

- 4) Is your product java-reliant – and if so – does it include java support – or does it have to be purchased separately from Oracle?

Fischer requires OPEN JDK for operating the Fischer solution.

- 5) Can your product be integrated with the major EMR suites and is there additional cost or set up needed that is not part of the core product?

If an EMR suite contains methods for integration, such as APIs, integration will be built as part of the delivery of the solution. More details around the specific availability would depend on the application.

- 6) Does your product support Attribute-based access control ABAC? If so, how does it handle this type of access control?

Note: **Attribute-based access control (ABAC) is an authorization model that evaluates attributes (or characteristics), rather than roles, to determine access. The purpose of ABAC is to protect objects such as data, network devices, and IT resources from unauthorized users and actions—those that don't have "approved" characteristics as defined by an organization's security policies.**

Fischer supports both RBAC and ABAC. Policy qualifications can be determined down to an attribute level ensuring that users receive the right access at the right time.



7) Does your product have an integrated Role Mining solution?

The Fischer product provides a role mining solution as a stand-alone service, however it is delivered as part of our product.

8) Can a relational database be treated as a source of identity data? – Yes

- a. Does the relational database schema need to conform to a specific standard? - No
 - i. If so, what is that standard?
- b. If not, is there a “mapping technology” that would allow someone with knowledge of the database schema to “map” database data objects to an IGA “standard” identity that can be stored in the IGA identity repository?

Fischer uses a JDBC connection to connect to the database. This allows us to extract data using queries for both tables and views.

- i. If a “mapping technology” exists, does the “mapping process” require custom code development, or can it be done via a visual interface and the “map” stored in a database or XML files and be referenced at runtime?
- ii. If there is no built-in “mapping technology”, what would be required to build a “mapper” between the database as identity data source and the IGA identity repository?

Fischer does not require a mapper for extracting data from a database. Our ETL engine has the necessary tools for manipulating the data as needed.

9) Can an XML file be treated as a source of identity data?

Yes

- a. Does the XML schema need to conform to a specific standard?
 - 1. If so, what is that standard?
- b. If not, is there a “mapping technology” that would allow someone with knowledge of the XML schema to “map” schema elements to an IGA “standard” identity that can be stored in the IGA identity repository?
- c. If a “mapping technology” exists, does the “mapping process” require custom code development, or can it be done via a visual interface and the “map” stored in a database or XML files and be referenced at runtime?
- d. If there is no built-in “mapping technology”, what would be required to build a “mapper” between the XML file as identity data source and the IGA identity repository?

10) Can a REST or SOAP web service that delivers payloads in JSON or XML format be treated as a source of identity data?

In the current version, Identity data cannot be introduced into the system via REST or SOAP. We are actively defining the APIs to enable this method of SoA intake.



- a. Does the web service need to conform to a specific standard, in terms of the structure of the data that it delivers?
 - i. If so, what is that standard?
- b. If not, is there a “mapping technology” that would allow someone with knowledge of the payload delivered by the web service to “map” payload data elements, whether the data format is JSON or XML, to an IGA “standard” identity that can be stored in the IGA identity repository?
 - i. If a “mapping technology” exists, does the “mapping process” require custom code development, or can it be done via a visual interface and the “map” stored in a database or XML files and be referenced at runtime?
- c. If there is no built-in “mapping technology”, what would be required to build a “mapper” between the payload data as identity data source and the IGA identity repository?

11) What other types of sources of identity data are supported, if any?

- a. What level of support is provided for each of those?

Fischer supports extracting data from a variety of target applications. If Fischer has a supported connector for a system it can be used as a source of identity data. This can be initiated from that target system or another system. Fischer allows for real-time lookups into other target systems for the purposes of extracting additional data that might be needed during the creation of an Identity.

12) Are identities submitted by different data sources retained for some period of time and then “merged” into the identity repository on a schedule?

All data pulled from a data source is retained in our staging table after being merged with other data sources. The staging table is then used to create the identity within Fischer.

- a. Can the retention time and merge schedule be adjusted as desired?

Retention of this data can be adjusted.

13) Are identities submitted by different data sources merged “on the fly” into the identity repository?

Fischer will merge different data sources at the time of processing. This data will be sent to the staging table to be pulled into Fischer as an Identity.

- a. If so, can identities submitted by each data source still be retained for some period of time, and is that retention time adjustable?

The merged identity will remain in the staging table and retained until no longer needed.

14) Is it possible to configure merging to be either on the fly or on a schedule for all data sources

Pulling data from a data source can be scheduled to run as needed. This can range from daily to every few minutes.



15) Is it possible to configure merging to be either on the fly or on a schedule for each data source independently?

Different processes would be built to extract data from the sources as needed. If different data sources have different rules for retrieving and merging data that would be considered a different process.

16) Under what conditions will identities from different data sources be automatically merged?

The institution controls the conditions for automatic merging of data. They will determine based the data being pulled what information is authoritative.

a. Can these conditions be adjusted for each data source, or must the same conditions apply to all data sources?

The conditions can be adjusted for each data source.

b. Do identity data elements need to match exactly (alpha case being irrelevant)?

Fischer can normalize the characters received and make the values uniformed case. This allows for comparison of the elements without having to be exact.

c. If identity data elements do not need to match exactly, can we specify the logic to be used for matching identity data elements?

Yes you can specify the logic used for matching identity data elements.

i. In particular, can we use phonetic spellings to match name parts?

Partial name resolution can be done to determine if a name closely resembles another name.

1. Can we add "weights" to identity data elements so that certain elements will be more deterministic for matching? –

The client determines which attributes to verify during the matching process. You can use multiple attributes for this purpose.

e. Can we create (or at least edit) the rules that specify which identity data elements will be used for matching?

Rules for matching are defined by the institution and can be adjusted as needed.

f. Can these rules differ, to some extent, for each identity data source?

Rules can differ for each data source.



- 17) Once identities have been automatically merged, is it possible for an IGA admin to “unmerge” the identities and then flag the newly unmerged identities so they will not be automatically merged again?

Specific workflow processes would be developed to manage the “unmerging” processes. These workflows would be initiated by an administrator of the solution and will split the identities and they will become independent identities at that point. The unique identifier should prevent any future merging.

- 18) When similar identities can't be automatically merged because of data differences, are these “slightly mismatching” identities flagged by the IGA for manual review?

- a. Is it possible for “slightly mismatching” identities to be manually merged by an IGA admin?

Workflow processes would be built to handle merging identities on an as needed basis. These workflows would be initiated by an administrator of the solution and would merge the identities and remove any, no longer needed, applications and access.

- b. If an admin determines that an identity submitted by a particular data source is “suspect”, can the admin “suspend” the “suspect” identity from being processed any further, such that it will not affect any identities store in the repository?

Fischer’s user match feature would allow the administrator to verify “suspect” identities to determine if they are the same identity or are unique.

- c. If an admin determines that a data source is submitting to many “suspect” identities, can the admin “suspend” receiving any new identities from the data source pending further investigation?

Suspending of workflows is built in the product. Once an issue is found, and administrator would simply suspend the workflow from executing until it is restarted.

- d. If “suspect” identities need to be purged from the system because it was determined they were submitted in error, can this be done?

This would be done through a utility workflow that would allow you to input the “suspected” identities and purge them from the system.

- e. If some of these “suspect” identities were already merged into the IGA identity repository, can they be “unmerged” from the repository by an admin?

Workflows would be created to handle instances where identities were merged and need to be unmerged. These workflows would be initiated by an administrator of the solution and would unmerge the accounts by creating the necessary new identity and provisioning the new identities resources.



- f. Can all identities from a “suspect” data source be unmerged from the repository back to the date and time when it was determined that the identities from that data source became “suspect”?

Fischer would unmerge the users back to a good state. It would use a workflow built for this specific purpose and would require a list of suspect identities in order to unmerge the corresponding identities.

19) Questions for Fisher:

- a. Does Fisher have Stage table format on what is stored for students and employees? Table definitions to see how it can be mapped with our data and what all changes has to be made to use it (aka data dictionary).

Yes. Fischer has the ability to map data elements to match your SoA and Identity needs. We do have pre-defined schema mappings, however your ability to design your data model is fully supported.

- b. Student data, can we add more attributes for them, can these be added into the staging and Fischer product for a student. Same for employees and faculty.

Fischer can store additional attributes about all user types. This data is stored in the identity profile.

- c. Can we have an automated approval process (Eg: library card) of the access request for a few and manual for others? Same for removing access based on end date.

Access requests can be automatically given to a user based on qualification to a policy or can be manually requested via Self-Service either by the user or a delegate. Approvals can be associated with both types.

- d. What programming language is the Fischer IGA written in?

Fischer is developed using Java.

- e. Policy list, is there a limit? Can this be loaded/migrated from current AD system in place.

There is no limit on the number of polices (roles) that can be managed by Fischer. Policies can be loaded from external sources such as AD.

- b. User Matching done only during automated provisioning, create new user and self-registration. What about bulk update on users and bulk delete of user, how will that be handled. (For example: summer high school students bulk update/delete).

User matching can be done for bulk users. Fischer’s user matching includes automated user creation, self-registration requests and delegated user accounts.



- c. Does Fischer have APIs to add/update/delete users and maybe policies as well?

Fischer has an API to update policies, which in turn can be used to drive updating users from an access point of view. Updating biographical information is accomplished by integrating with end points where the data sits at rest and detecting changes and driving change to Identity.

- d. Is there a way to manage what all a user can request for based on department number or title/job code. For example, all users with programming related position in Department X can request access to a code repository.

Yes, Fischer can present request able resources to a user based on type or other attribute data such as department, title, location, etc. This means that Students could get a different list of resources then staff or faculty.



Fischer International Identity, LLC Maintenance and Support for UC System RFP No #002197-SEP2020

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 % of the license charge. See attached Price Quote.

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.

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. All unplanned outage events are communicated through mass ticket generation by Fischer when identified. The tickets are then updated when service is restored. For planned maintenance windows, Fischer publishes an annual calendar of all maintenance activities. Additionally, automated maintenance reminder notifications are sent 14 days prior to the planned maintenance window.

The levels of service provided by Fischer to Licensee 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 Licensee 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 Licensee 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

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 in 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

Attachment B to Exhibit 1

**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.

4. DISCRETIONARY SERVICES HOURS

- 4.1. Each IaaS® subscription includes a number of monthly services hours so that “routine” administrative tasks/solution adjustments can be made to an accepted production solution without the Client incurring additional costs. These services may be used at the client’s discretion according to the guidelines below.
 - 4.1.1. The number of Discretionary Services hours is based on the modules licensed. The maximum number of monthly hours is ten (10) regardless of the number of module/services licensed.
 - 4.1.2. Discretionary Services hours can be applied ONLY to the Client’s accepted production solution. Hours cannot be applied to deliver “new” functionality that has not been previously delivered and accepted.
 - 4.1.2.1. VALID activities include: changing an existing workflow, updating an IP address of target system, adding provisioning policies (provided that all required attributes and workflows are already available within the solution), troubleshooting problems that are determined to be the responsibility of the Client (note: the Client is not charged for troubleshooting issues that are the result of a defect)
 - 4.1.2.2. INVALID activities include: analysis of Client requirements, adding a new system or resource, creating new workflows, adding newly-licensed IdM

capabilities/services

- 4.1.3. Clients must identify one or more named persons as authorized to approve all Work Orders related to Discretionary Services. If preferred, the Client may have two classes of authorized persons: one that can approve Work Orders with a financial cost, and one that can approve only Work Orders that can be performed within the remaining number of hours for the current month.
- 4.1.4. Any project that exceeds the monthly allowance will be billed at Fischer's standard Operations Services hourly rate and only upon written approval by the Client. Notes: discretionary hours cannot be aggregated across multiple months (e.g., cannot combine 2 months worth of discretionary hours to avoid costs) projects are billed against the current month's discretionary hours, regardless of when the work is actually performed (e.g., a 16-hour project approved in August will be billed against August hours even if some or all of the work is performed in September or later months)
- 4.1.5. Projects are billed in increments of 1 hour.

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"> • Being the point of contact for Authorized Client Representatives related to all software issues and changes (bugs, usability questions and enhancements). • Collaborating with an Authorized Client Representatives to establish the priority of support requests. • Answering questions about the functionality of the software. • Performing initial troubleshooting and providing known, documented fixes or workarounds when available. • Recording support requests, opening support tickets and assigning ticket numbers • Tracking the status of support tickets.

	<ul style="list-style-type: none"> • Transitioning support requests to Level-2 Technical Support when required. • Communicating problem resolution to Authorized Client Representatives.
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"> • Conducting root-cause analysis to determine whether a problem is caused by the configuration or by an underlying software issue. • Transitioning problems to the appropriate Level-3 Technical Lead as required via the terms stated in Section V SUPPORT REQUESTS AND PRIORITY LEVELS. • Communicating problem resolution to Authorized Client Representatives.
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"> • Leading the programming and quality assurance efforts for any coding and testing required to resolve software problems. • Delivering workarounds for software errors that cannot be resolved rapidly. • Communicate problem resolution to Level-2 Specialists. <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)
Business and financial exposure			
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.
Work Outage			
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.
Number of Covered Persons Affected			
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.
Timing of Usage			
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.
Workaround [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).
Response Time to Conduct Initial Conversation			
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

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 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
Priority 4 (Low)	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.



Attachment C to Exhibit 1

Fischer International Identity, LLC Training Options for UC System RFP No #002197-SEP2020

Fischer Identity provides onsite training 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.

All customer training and the associated material is created based on the specific design and functionality of the customer's solution. We utilize members of our Implementation and Solution Management teams to perform the training. Each team member has extensive knowledge of the Fischer product and have all facilitated training sessions with our customers. Fischer Product guides and solution documentation are provided as part of the training.

Topic covered in basic training include: Managing Approvals; Adding Policies and Roles, Configuring Password management. Topic covered in advanced training include: Applying Patches and Managing Workflow Processes.

For end users, Fischer offers "train the trainer" courses based on the modules being utilized. This approach allows your staff to train the user population as needed and typically reviews all end user interfaces your users will encounter.

Fischer also offer the Fischer Identity Guru Training Program for customer who would like to purchase additional training.

Training Programs	Location	Fee**	Seats	Description
Online, self-paced program	Virtual	\$2,500.00	Unlimited	Unlimited Licensed Users and 24x7 access to Fischer's Guru training platform.
Paradise Program	Naples, FL	\$4,500.00	per Seat, max of 10***	Requires registration, fixed dates during the year and is open to all customers. Fischer would provide the lab environment necessary to commence training. Attendees would be required to bring a laptop to access the training lab. This training is limited to 10 attendees. There will be a schedule published annually for registration.

1.

Customized Training Tracks*	\$10,000.00	5 full days of training at customer facilities. Fischer would provide the lab environment necessary to commence training. Attendees would be required to bring a laptop to access the training lab.		
------------------------------------	--------------------	--	--	--

2.

General Overview & Implementation Training	Customer premises	max 10 attendees	This course will provide participants with an overview of "How Fischer Works" and focus on how to implement an end to end solution Identity Governance & Administration solution leveraging the Fischer Identity Suite.	
Fischer Administration & Solution Mgt. Training	Customer premises	max 10 attendees	This course will provide participants with a detailed review of the Administrative user interface as well as troubleshooting techniques and ongoing change control of your Fischer IGA solution.	

1



Attachment C to Exhibit 1

Infrastructure Training	Customer premises	max 10 attendees	This course will provide participants with the know-how to install, configure and prepare the Fischer IGA Suite for Implementation and Production. This will include best practices around constructing your infrastructure as well as ongoing maintenance and monitoring solutions.
-------------------------	-------------------	------------------	--

Virtual Training Options

"I Got This" wiki access only	Virtual	\$300.00	per Seat	Per user access to Fischer Central. This would provide an individual seat for Fischer's wiki to keep up to date with the latest training content in digital form.
"Just print me the guides" PDF Guides	N/A	\$0.00	NA	If the customer chooses this model, Fischer will provide PDF of all current content for the trainee to review. Fischer will also offer access the assessments free of charge.

*Customized training can be extended to unlimited attendees for an additional \$5,000.

** Travel & Expense is not included in the Fee and would be billed separate.

***2 or more attendees from a single customer will result in a 20% discount per seat for the Paradise Program

Fischer Identity offers both basic and advanced training. For customers administering their own solution, Fischer offers week-long Basic and Advanced Fischer Identity training courses for administrators. This can be held onsite, remotely through web-conference or at the Fischer Corporate Headquarters in Naples, FL. The training agenda is created for your solution, covering all areas your staff will need to understand how the product is integrated and deployed. Topic covered in basic training include: Managing Approvals, Adding policies roles, and Configuring Password management. Topic covered in advanced training include: Applying Patches and managing workflow processes. This training can be done either at your location or at the Fischer corporate headquarters in Naples Florida. T&E will apply.

For customers with Identity as a Servicer cloud subscriptions, Fischer offers "train the trainer" courses based on the modules being utilized. This approach allows your staff to train the user population as needed and typically reviews all end user interfaces your users will encounter. This training is typically delivered remotely due to its short duration; however, training can be done at your location if preferred. T&E will apply.

There are no industry certifications directly related to Identity Access Management.

Fischer Identity offers a comprehensive training & certification platform called the Identity GURU program. This program focuses not only on training but certifying resources to ensure that they have an understanding of the typical Identity and Access Management IAM challenges facing organization today but also offers a complete 360 degree view of the Fischer Identity platform and its flexible deployment model. All training is available via our cost effective yearly subscription model. This model allows customers to tailor their training needs to meet their desired business objectives.

We offer the following training experiences:

Fischer University - Online courses and learning tracks that are focused on understanding Identity and Access Management, and understanding the capabilities, solution implementation and management of the Fischer Identity platform.

Paradise Program - Classroom based training located at our Naples based headquarters. Sessions are scheduled to minimize the impact to the day to day job responsibilities of the attendees. These sessions are a focused, in-depth review of the content available on the Fischer University.



Attachment C to Exhibit 1

Customer Specific - Training agendas are tailored to meet a customer's specific objectives and are held onsite at a location of their choosing.

Best Practices - Business Analysis workshop that help customers focus on high-level solution requirements and the development of an IAM roadmap for the implementation of their IAM requirements and business objectives.

Customers can consume the above training in one of the following subscription levels, these levels allow customers to choose the types of training required for their users:

Basic - All available online Fischer University content.

Intermediate - Basic Level + Paradise Program

Advanced - Intermediate Level + Customer Specific

Platinum - Advanced Level + Best Practices

Once subscribed, customers are allocated an appropriate number of seats based on the level chosen. If additional seats are required, they can be allocated for an additional charge.

OMNIA PARTNERS EXHIBITS
EXHIBIT A- RESPONSE FOR NATIONAL COOPERATIVE CONTRACT

1.0 Scope of National Cooperative Contract

Capitalized terms not otherwise defined herein shall have the meanings given to them in the Master Agreement or in the Administration Agreement between Supplier and OMNIA Partners.

1.1 Requirement

The University of California (hereinafter defined and referred to as “Principal Procurement Agency”), on behalf of itself and the National Intergovernmental Purchasing Alliance Company, a Delaware corporation d/b/a OMNIA Partners, Public Sector (“**OMNIA Partners**”), is requesting proposals for IT Security Tools. The intent of this Request for Proposal is any contract between Principal Procurement Agency and Supplier resulting from this Request for Proposal (“**Master Agreement**”) be made available to other public agencies nationally, including state and local governmental entities, public and private primary, secondary and higher education entities, non-profit entities, and agencies for the public benefit (“**Public Agencies**”), through OMNIA Partners’ cooperative purchasing program. The Principal Procurement Agency has executed a Principal Procurement Agency Certificate with OMNIA Partners, an example of which is included as Exhibit D, and has agreed to pursue the Master Agreement. Use of the Master Agreement by any Public Agency is preceded by their registration with OMNIA Partners as a Participating Public Agency in OMNIA Partners’ cooperative purchasing program. Registration with OMNIA Partners as a Participating Public Agency is accomplished by Public Agencies entering into a Master Intergovernmental Cooperative Purchasing Agreement, an example of which is attached as Exhibit C, and by using the Master Agreement, any such Participating Public Agency agrees that it is registered with OMNIA Partners, whether pursuant to the terms of the Master Intergovernmental Purchasing Cooperative Agreement or as otherwise agreed to. The terms and pricing established in the resulting Master Agreement between the Supplier and the Principal Procurement Agency will be the same as that available to Participating Public Agencies through OMNIA Partners.

All transactions, purchase orders, invoices, payments etc., will occur directly between the Supplier and each Participating Public Agency individually, and neither OMNIA Partners, any Principal Procurement Agency nor any Participating Public Agency, including their respective agents, directors, employees or representatives, shall be liable to Supplier for any acts, liabilities, damages, etc., incurred by any other Participating Public Agency. Supplier is responsible for knowing the tax laws in each state.

This Exhibit A defines the expectations for qualifying Suppliers based on OMNIA Partners’ requirements to market the resulting Master Agreement nationally to Public Agencies. Each section in this Exhibit A refers to the capabilities, requirements, obligations, and prohibitions of competing Suppliers on a national level in order to serve Participating Public Agencies through OMNIA Partners.

These requirements are incorporated into and are considered an integral part of this RFP. OMNIA Partners reserves the right to determine whether or not to make the Master Agreement awarded by the Principal Procurement Agency available to Participating Public Agencies, in its sole and absolute discretion, and any party submitting a response to this RFP acknowledges that any award

OMNIA PARTNERS EXHIBITS
EXHIBIT A- RESPONSE FOR NATIONAL COOPERATIVE CONTRACT

by the Principal Procurement Agency does not obligate OMNIA Partners to make the Master Agreement available to Participating Procurement Agencies.

1.2 Marketing , Sales and Administrative Support

During the term of the Master Agreement OMNIA Partners intends to provide marketing, sales, partnership development and administrative support for Supplier pursuant to this section that directly promotes the Supplier's products and services to Participating Public Agencies through multiple channels, each designed to promote specific products and services to Public Agencies on a national basis.

OMNIA Partners will assign the Supplier a Director of Partner Development who will serve as the main point of contact for the Supplier and will be responsible for managing the overall relationship between the Supplier and OMNIA Partners. The Director of Partner Development will work with the Supplier to develop a comprehensive strategy to promote the Master Agreement and will connect the Supplier with appropriate stakeholders within OMNIA Partners including, Sales, Marketing, Contracting, Training, Operations & Support.

The OMNIA Partners marketing team will work in conjunction with Supplier to promote the Master Agreement to both existing Participating Public Agencies and prospective Public Agencies through channels that may include:

- A. Marketing collateral (print, electronic, email, presentations)
- B. Website
- C. Trade shows/conferences/meetings
- D. Advertising
- E. Social Media

The OMNIA Partners sales teams will work in conjunction with Supplier to promote the Master Agreement to both existing Participating Public Agencies and prospective Public Agencies through initiatives that may include:

- A. Individual sales calls
- B. Joint sales calls
- C. Communications/customer service
- D. Training sessions for Public Agency teams
- E. Training sessions for Supplier teams

The OMNIA Partners contracting teams will work in conjunction with Supplier to promote the Master Agreement to both existing Participating Public Agencies and prospective Public Agencies through:

OMNIA PARTNERS EXHIBITS
EXHIBIT A- RESPONSE FOR NATIONAL COOPERATIVE CONTRACT

- A. Serving as the subject matter expert for questions regarding joint powers authority and state statutes and regulations for cooperative purchasing
- B. Training sessions for Public Agency teams
- C. Training sessions for Supplier teams
- D. Regular business reviews to monitor program success
- E. General contract administration

1.3 Estimated Volume

The dollar volume purchased under the Master Agreement is estimated to be approximately__ million annually. While no minimum volume is guaranteed to Supplier, the estimated annual volume is projected based on the current annual volumes among the Principal Procurement Agency, other Participating Public Agencies that are anticipated to utilize the resulting Master Agreement to be made available to them through OMNIA Partners, and volume growth into other Public Agencies through a coordinated marketing approach between Supplier and OMNIA Partners.

1.4 Award Basis

The basis of any contract award resulting from this RFP made by Principal Procurement Agency will, at OMNIA Partners option, be the basis of award on a national level through OMNIA Partners. If multiple Suppliers are awarded by Principal Procurement Agency under the Master Agreement, those same Suppliers will be required to extend the Master Agreement to Participating Public Agencies through OMNIA Partners. Utilization of the Master Agreement by Participating Public Agencies will be at the discretion of the individual Participating Public Agency. Certain terms of the Master Agreement specifically applicable to the Principal Procurement Agency (e.g. governing law) are subject to modification for each Participating Public Agency as Supplier, such Participating Public Agency and OMNIA Partners shall agree without being in conflict with the Master Agreement. Participating Agencies may request to enter into a separate supplemental agreement to further define the level of service requirements over and above the minimum defined in the Master Agreement (i.e. invoice requirements, order requirements, specialized delivery, diversity requirements such as minority and woman owned businesses, historically underutilized business, governing law, etc.). It shall be the responsibility of the Supplier to comply, when applicable, with the prevailing wage legislation in effect in the jurisdiction of the Participating Agency. It shall further be the responsibility of the Supplier to monitor the prevailing wage rates as established by the appropriate department of labor for any increase in rates during the term of the Master Agreement and adjust wage rates accordingly. Any supplemental agreement developed as a result of the Master Agreement is exclusively between the Participating Agency and the Supplier (Contract Sales are reported to OMNIA Partners).

OMNIA PARTNERS EXHIBITS
EXHIBIT A- RESPONSE FOR NATIONAL COOPERATIVE CONTRACT

All purchase orders issued and accepted by the Supplier may survive expiration or termination of the Master Agreement. Participating Agencies' purchase orders may exceed the term of the Master Agreement if the purchase order is issued prior to the expiration of the Master Agreement. Supplier is responsible for reporting all sales and paying the applicable administrative fee for sales that use the Master Agreement as the basis for the purchase order, even though Master Agreement may have expired.

1.5 Objectives of Cooperative Program

This RFP is intended to achieve the following objectives regarding availability through OMNIA Partners' cooperative program:

- A. Provide a comprehensive competitively solicited and awarded national agreement offering the Products covered by this solicitation to Participating Public Agencies;
- B. Establish the Master Agreement as the Supplier's primary go to market strategy to Public Agencies nationwide;
- C. Achieve cost savings for Supplier and Public Agencies through a single solicitation process that will reduce the Supplier's need to respond to multiple solicitations and Public Agencies need to conduct their own solicitation process;
- D. Combine the aggregate purchasing volumes of Participating Public Agencies to achieve cost effective pricing.

2.0 REPRESENTATIONS AND COVENANTS

As a condition to Supplier entering into the Master Agreement, which would be available to all Public Agencies, Supplier must make certain representations, warranties and covenants to both the Principal Procurement Agency and OMNIA Partners designed to ensure the success of the Master Agreement for all Participating Public Agencies as well as the Supplier.

2.1 Corporate Commitment

Supplier commits that (1) the Master Agreement has received all necessary corporate authorizations and support of the Supplier's executive management, (2) the Master Agreement is Supplier's primary "go to market" strategy for Public Agencies, (3) the Master Agreement will be promoted to all Public Agencies, including any existing customers, and Supplier will transition existing customers, upon their request, to the Master Agreement, and (4) that the Supplier has read and agrees to the terms and conditions of the Administration Agreement with OMNIA Partners and will execute such agreement concurrent with and as a condition of its execution of the Master Agreement with the Principal Procurement Agency. Supplier will identify an executive corporate sponsor and a separate national account manager within the RFP response that will be responsible for the overall management of the Master Agreement.

OMNIA PARTNERS EXHIBITS
EXHIBIT A- RESPONSE FOR NATIONAL COOPERATIVE CONTRACT

2.2 Pricing Commitment

Supplier commits the not-to-exceed pricing provided under the Master Agreement pricing is its lowest available (net to buyer) to Public Agencies nationwide and further commits that if a Participating Public Agency is eligible for lower pricing through a national, state, regional or local or cooperative contract, the Supplier will match such lower pricing to that Participating Public Agency under the Master Agreement.

2.3 Sales Commitment

Supplier commits to aggressively market the Master Agreement as its go to market strategy in this defined sector and that its sales force will be trained, engaged and committed to offering the Master Agreement to Public Agencies through OMNIA Partners nationwide. Supplier commits that all Master Agreement sales will be accurately and timely reported to OMNIA Partners in accordance with the OMNIA Partners Administration Agreement. Supplier also commits its sales force will be compensated, including sales incentives, for sales to Public Agencies under the Master Agreement in a consistent or better manner compared to sales to Public Agencies if the Supplier were not awarded the Master Agreement.

3.0 SUPPLIER RESPONSE

Supplier must supply the following information in order for the Principal Procurement Agency to determine Supplier's qualifications to extend the resulting Master Agreement to Participating Public Agencies through OMNIA Partners.

3.1 Company

A. Brief history and description of Supplier.

Fischer is the number one provider of Identity Management Services for Higher Education. Over 100 campuses use Fischer Identity products and services, with many more planning to leverage their same success.

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.

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.

OMNIA PARTNERS EXHIBITS
EXHIBIT A- RESPONSE FOR NATIONAL COOPERATIVE CONTRACT

In 2005, Fischer has 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, and 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 then 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, 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 the only solely focused Identify Governance and Administration vendor that is an Ellucian Alliance Partner. 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 Identity 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 Identity.

B. Total number and location of sales persons employed by Supplier.

Sales resources: (all with multiple years of experience with IGA and Higher Education).

- **Janet Yarbrough**, Director of West Region and Partner Development;
- **Greg Berg**, Director of Midwest Region;
- **Gary J. O'Neill**, Director of South and Mid-Atlantic Region;
- **Robertt McEwan**, Director of Northeast Region;
- **Matt Dudonis**, Director Sales Engineering;
- Bryan Leber, Director Professional Services,
- John Heuring, Director of Operations.

Additionally, both Andrew Sroka, CEO Fischer Identity and Dan Dagnall, COO Fischer Identity are engaged with the efforts in the UC System and CSU System.

Fischer also has a partner community with expertise in Identity Management. A few examples of Fischer's partners include IDMWORKS, Identropy, Formmi and a distributor channel, Synnex. All of these companies have nationwide coverage.

OMNIA PARTNERS EXHIBITS
EXHIBIT A- RESPONSE FOR NATIONAL COOPERATIVE CONTRACT

C.Number and location of support centers (if applicable) and location of corporate office.

Fischer has 7 full-time support staff available Monday through Friday, 24 hours per day. Incidents categorized as Priority 1 and Priority 2 are monitored 24 hours, 7 days per week, including vendor holidays.

Fischer's corporate headquarters is located in Naples, FL

D. Annual sales for the three previous fiscal years.

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 offer the following indicators:

Financial Metrics:

3 year increases March 2016 - March 2019

- Gross Sales: 70%
- Average Contract Value ACV: 7%
- New Customer Accounts: 60%

Human Capital:

- 3 year employee base growth: 26%
- CEO tenure: Andrew Sroka joined Fischer in 1998
- Approximately 69% of Fischer's workforce is devoted to software development and quality assurance

Workforce Dept:

- Research & Development: 30%
- Sales/Marketing: 17%
- Customer Support & Services: 50%
- Administrative: 3%

Assurances:

- Escrow: Fischer will escrow source code for on-premises 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.

E. Submit FEIN and Dunn & Bradstreet report.

Identity is 20-5385349.

See Attachment A - Dun & Bradstreet Report

OMNIA PARTNERS EXHIBITS
EXHIBIT A- RESPONSE FOR NATIONAL COOPERATIVE CONTRACT

F. Describe any green or environmental initiatives or policies.

N/A

G. Describe any diversity programs or partners supplier does business with and how Participating Agencies may use diverse partners through the Master Agreement. Indicate how, if at all, pricing changes when using the diversity program.

None

H. Describe any historically underutilized business certifications supplier holds and the certifying agency. This may include business enterprises such as minority and women owned, small or disadvantaged, disable veterans, etc.

None

I. Describe how supplier differentiates itself from its competitors.

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.

Fischer's Workflow and Connectivity Studio - Our Workflow and Connectivity Studios is where we truly differentiate ourselves from the competition. We have abstracted the coding layer a zero-coding approach to building workflows. You do not need to be an expert in any programming or scripting language, rather we have normalized the skillset required to build enterprise grade identity management workflows. Our studio provides visual tools, intuitive design and data mapping functionality, connectivity and schema discovery in a visual drag and drop WYSIWYG usability to build complex workflows without the traditional coding or scripting required in other identity systems. To accompany this Fischer provides templates and schemas that we have developed and deployed over time in other institutions to expedite delivery. .

Higher Education specialization -

- Fischer is the number one provider of Identity Management Services for Higher Education. Over 100 campuses use Fischer Identity products and services, with many more planning to leverage their same success.
- We understand higher education processes, systems/technical environments, users, business challenges, goals, and missions.
- Choice of Deployment Model: on-campus software or hosted cloud subscription.
- Ease and Speed to change and extend the solution to meet new business requirements.
- Higher Education Experience: Fischer has over 10 years of experience in cloud based Identity Access Management.
- 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.

J. Describe any present or past litigation, bankruptcy or reorganization involving supplier.

None

K. Felony Conviction Notice: Indicate if the supplier

- a. is a publicly held corporation and this reporting requirement is not applicable;

OMNIA PARTNERS EXHIBITS
EXHIBIT A- RESPONSE FOR NATIONAL COOPERATIVE CONTRACT

- b. is not owned or operated by anyone who has been convicted of a felony; or
- c. is owned or operated by and individual(s) who has been convicted of a felony and provide the names and convictions.

Is not owned or operated by anyone who has been convicted of a felony.

- L. Describe any debarment or suspension actions taken against supplier

None

3.2 Distribution, Logistics

- A. Describe the full line of products and services offered by supplier.

- B. Describe how supplier proposes to distribute the products/service nationwide. Include any states where products and services will not be offered under the Master Agreement, including U.S. Territories and Outlying Areas.

Products will be distributed directly through Fischer Identity.

- C. Describe how Participating Agencies are ensure they will receive the Master Agreement pricing; include all distribution channels such as direct ordering, retail or in-store locations, through distributors, etc. Describe how Participating Agencies verify and audit pricing to ensure its compliance with the Master Agreement.

The agreement will be directly between Fischer Identity, OMNIA Partners and the UC System

- D. Identify all other companies that will be involved in processing, handling or shipping the products/service to the end user.

Fischer will be the sole agency responsible for providing products/services to the end user.

- E. Provide the number, size and location of Supplier's distribution facilities, warehouses and retail network as applicable.

Fischer does not require a warehouse of distribution facility this is an electronically delivered software.

3.3 Marketing and Sales

- A. Provide a detailed ninety-day plan beginning from award date of the Master Agreement describing the strategy to immediately implement the Master Agreement as supplier's primary go to market strategy for Public Agencies to supplier's teams nationwide, to include, but not limited to:

OMNIA PARTNERS EXHIBITS
EXHIBIT A- RESPONSE FOR NATIONAL COOPERATIVE CONTRACT

Fischer Identity and OMNIA Partners will develop a mutually collaborative plan developed upon award.

- i. Executive leadership endorsement and sponsorship of the award as the public sector go-to-market strategy within first 10 days

The endorsement would be provided by our CEO, R. Andrew Sroka.

- ii. Training and education of Supplier’s national sales force with participation from the Supplier’s executive leadership, along with the OMNIA Partners team within first 90 days

We have a well developed training curriculum which will be made available as appropriate.

Fischer offers 3 training methods that you can choose from that best fits the training needs of your organization:

- **On Demand Web-Based LMS Courses**
 - Our web-based training courses covers the entire Fischer product, including but not limited to, comprehensive walkthroughs of configuring product features, IGA best practices, and troubleshooting. The web-based training is available 24 hours a day, 7 days a week. The content within the courses has closed captioning.

- **Quarterly Training Workshops**
 - In this model, Fischer invites all of our customers to join our quarterly, collaborative training on the Fischer product.

- **Dedicated Training Workshops**
 - The dedicated training workshop entails a member of the Fischer team to train your specific organization. Under this approach, a member of the Fischer team can perform training on-site at your location or we can host the dedicated training workshop at our headquarters location in Naples, Florida.

Fischer also offer the Fischer Identity Guru Training Program for customer who would like to purchase additional training.

Training Programs	Location	Fee**	Seats	Description
-------------------	----------	-------	-------	-------------

OMNIA PARTNERS EXHIBITS
EXHIBIT A- RESPONSE FOR NATIONAL COOPERATIVE CONTRACT

Online, self-paced program	Virtual	\$2,500.00	Unlimited	Unlimited Licensed Users and 24x7 access to Fischer's Guru training platform.
Paradise Program	Naples, FL	\$4,500.00	per Seat, max of 10***	Requires registration, fixed dates during the year and is open to all customers. Fischer would provide the lab environment necessary to commence training. Attendees would be required to bring a laptop to access the training lab. This training is limited to 10 attendees. There will be a schedule published annually for registration.

Customized Training Tracks*		\$10,000.00		5 full days of training at customer facilities. Fischer would provide the lab environment necessary to commence training. Attendees would be required to bring a laptop to access the training lab.
------------------------------------	--	--------------------	--	--

General Overview & Implementation Training	Customer premises		max 10 attendees	This course will provide participants with an overview of "How Fischer Works" and focus on how to implement an end to end solution Identity Governance & Administration solution leveraging the Fischer Identity Suite.
Fischer Administration & Solution Mgt. Training	Customer premises		max 10 attendees	This course will provide participants with a detailed review of the Administrative user interface as well as troubleshooting techniques and ongoing change control of your Fischer IGA solution.
Infrastructure Training	Customer premises		max 10 attendees	This course will provide participants with the know-how to install, configure and prepare the Fischer IGA Suite for Implementation and Production. This will include best practices around constructing your infrastructure as well as ongoing maintenance and monitoring solutions.

Virtual Training Options

"I Got This" wiki access only	Virtual	\$300.00	per Seat	Per user access to Fischer Central. This would provide an individual seat for Fischer's wiki to keep up to date with the latest training content in digital form.
-------------------------------	---------	----------	----------	---

OMNIA PARTNERS EXHIBITS
EXHIBIT A- RESPONSE FOR NATIONAL COOPERATIVE CONTRACT

"Just print me the guides" PDF Guides	N/A	\$0.00	NA	If the customer chooses this model, Fischer will provide PDF of all current content for the trainee to review. Fischer will also offer access the assessments free of charge.
---------------------------------------	-----	--------	----	---

- *Customized training can be extended to unlimited attendees for an additional \$5,000.
- ** Travel & Expense is not included in the Fee and would be billed separate.
- ***2 or more attendees from a single customer will result in a 20% discount per seat for the Paradise Program

B. Provide a detailed ninety-day plan beginning from award date of the Master Agreement describing the strategy to market the Master Agreement to current Participating Public Agencies, existing Public Agency customers of Supplier, as well as to prospective Public Agencies nationwide immediately upon award, to include, but not limited to:

- i. Creation and distribution of a co-branded press release to trade publications
- ii. Announcement, Master Agreement details and contact information published on the Supplier’s website within first 90 days
- iii. Design, publication and distribution of co-branded marketing materials within first 90 days
- iv. Commitment to attendance and participation with OMNIA Partners at national (i.e. NIGP Annual Forum, NPI Conference, etc.), regional (i.e. Regional NIGP Chapter Meetings, Regional Cooperative Summits, etc.) and supplier-specific trade shows, conferences and meetings throughout the term of the Master Agreement
- v. Commitment to attend, exhibit and participate at the NIGP Annual Forum in an area reserved by OMNIA Partners for partner suppliers. Booth space will be purchased and staffed by Supplier. In addition, Supplier commits to provide reasonable assistance to the overall promotion and marketing efforts for the NIGP Annual Forum, as directed by OMNIA Partners.
- vi. Design and publication of national and regional advertising in trade publications throughout the term of the Master Agreement
- vii. Ongoing marketing and promotion of the Master Agreement throughout its term (case studies, collateral pieces, presentations, promotions, etc.)
- viii. Dedicated OMNIA Partners internet web-based homepage on Supplier’s website with:
 - OMNIA Partners standard logo;
 - Copy of original Request for Proposal;
 - Copy of Master Agreement and amendments between Principal Procurement Agency and Supplier;
 - Summary of Products and pricing;
 - Marketing Materials
 - Electronic link to OMNIA Partners’ website including the online registration page;

OMNIA PARTNERS EXHIBITS
EXHIBIT A- RESPONSE FOR NATIONAL COOPERATIVE CONTRACT

- A dedicated toll-free number and email address for OMNIA Partners

C. Describe how Supplier will transition any existing Public Agency customers' accounts to the Master Agreement available nationally through OMNIA Partners. Include a list of current cooperative contracts (regional and national) Supplier holds and describe how the Master Agreement will be positioned among the other cooperative agreements.

We will collaborate with OMNIA Partners on any existing opportunities. All opportunities will be mutually identified and addressed.

D. Acknowledge Supplier agrees to provide its logo(s) to OMNIA Partners and agrees to provide permission for reproduction of such logo in marketing communications and promotions. Acknowledge that use of OMNIA Partners logo will require permission for reproduction, as well.

Agreed

E. Confirm Supplier will be proactive in direct sales of Supplier's goods and services to Public Agencies nationwide and the timely follow up to leads established by OMNIA Partners. All sales materials are to use the OMNIA Partners logo. At a minimum, the Supplier's sales initiatives should communicate:

- i. Master Agreement was competitively solicited and publicly awarded by a Principal Procurement Agency
- ii. Best government pricing
- iii. No cost to participate
- iv. Non-exclusive

Agreed

F. Confirm Supplier will train its national sales force on the Master Agreement. At a minimum, sales training should include:

- i. Key features of Master Agreement
- ii. Working knowledge of the solicitation process
- iii. Awareness of the range of Public Agencies that can utilize the Master Agreement through OMNIA Partners
- iv. Knowledge of benefits of the use of cooperative contracts

Agreed

OMNIA PARTNERS EXHIBITS
EXHIBIT A- RESPONSE FOR NATIONAL COOPERATIVE CONTRACT

G. Provide the name, title, email and phone number for the person(s), who will be responsible for:

i. Executive Support

R. Andrew Sroka
andrew.s@fischeridentity.com
239 643-1500

ii. Marketing

Adrienn Wiebe
adrienn.w@fischeridentity.com
239 436-2507

iii. Sales

Janet Yarbrough
janet.y@fischeridentity.com
303 589-5435

iv. Sales Support

Matt Dudonis
matt.d@fischeridentity.com
239 436-2772

v. Financial Reporting

Jonah Dooley
Jonah.d@fischeridentity.com
239 436-2731

vi. Accounts Payable

Jonah Dooley
Jonah.d@fischeridentity.com
239 436-2731

OMNIA PARTNERS EXHIBITS
EXHIBIT A- RESPONSE FOR NATIONAL COOPERATIVE CONTRACT

vii. Contracts

R. Andrew Sroka
andrew.s@fischeridentity.com
239 643-1500

H. Describe in detail how Supplier's national sales force is structured, including contact information for the highest-level executive in charge of the sales team.

Fischer International Identity, LLC Support/Sales Network for UC System RFP No #002197-SEP2020

Fischer has 4 Sales Directors:

Janet Yarbrough
Sales Director West
Phone: (303) 589-5435
email: janet.y@fischeridentity.com

Gary J. O'Neill
Sales Director Southwest
Phone: (678) 366-0426
Email: gary.o@fischeridentity.com

Robert McEwen
Sales Director, Northeast
Phone: (732) 775-0045
Email: robert.m@fischeridentity.com

Greg Berg
Sales Director, Midwest
Phone: (469) 418-4777
Email: greg.b@fischeridentity.com

Fischer has a network of integrators and resellers visit our website at:
<https://www.fischeridentity.com/partners/>

I. Explain in detail how Supplier will manage the overall national program throughout the term of the Master Agreement, including ongoing coordination of marketing and sales efforts, timely new Participating Public Agency account set-up, timely contract administration, etc.

Plan will be developed in collaboration with OMNIA Partners upon contract award

OMNIA PARTNERS EXHIBITS
EXHIBIT A- RESPONSE FOR NATIONAL COOPERATIVE CONTRACT

J.State the amount of Supplier’s Public Agency sales for the previous fiscal year. Provide a list of Supplier’s top 10 Public Agency customers, the total purchases for each for the previous fiscal year along with a key contact for each.

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.

K.Describe Supplier’s information systems capabilities and limitations regarding order management through receipt of payment, including description of multiple platforms that may be used for any of these functions.

L.Not Applicable

M.If the Supplier wants to guarantee sales, provide the Contract Sales (as defined in Section 10 of the National Intergovernmental Purchasing Alliance Company Administration Agreement) that Supplier will guarantee each year under the Master Agreement for the initial three years of the Master Agreement (“Guaranteed Contract Sales”).

\$_____.00 in year one
\$_____.00 in year two
\$_____.00 in year three

To the extent Supplier guarantees minimum Contract Sales, the administration fee shall be calculated based on the greater of the actual Contract Sales and the Guaranteed Contract Sales.

N. Even though it is anticipated many Public Agencies will be able to utilize the Master Agreement without further formal solicitation, there may be circumstances where Public Agencies will issue their own solicitations. The following options are available when responding to a solicitation for Products covered under the Master Agreement.

We will address each opportunity on an individual case by case basis determining the best pricing strategy and overall approach in conjunction with OMNIA Partners.

- i. Respond with Master Agreement pricing (Contract Sales reported to OMNIA Partners).
- ii. If competitive conditions require pricing lower than the standard Master Agreement not-to-exceed pricing, Supplier may respond with lower pricing through the Master Agreement. If Supplier is awarded the contract, the sales are reported as Contract Sales to OMNIA Partners under the Master Agreement.
- iii. Respond with pricing higher than Master Agreement only in the unlikely event that the Public Agency refuses to utilize Master Agreement (Contract Sales are not reported to OMNIA Partners).
- iv. If alternative or multiple proposals are permitted, respond with pricing higher than Master Agreement, and include Master Agreement as the alternate or additional proposal.

OMNIA PARTNERS EXHIBITS
EXHIBIT A- RESPONSE FOR NATIONAL COOPERATIVE CONTRACT

We will address each opportunity on an individual case by case basis determining the best pricing strategy and overall approach in conjunction with OMNIA Partners.

Detail Supplier's strategies under these options when responding to a solicitation.

We will develop an overall strategic plan coupled with individual opportunity plans; developed in collaboration with OMNIA Partners based upon specific opportunities.

OMNIA PARTNERS EXHIBITS
EXHIBIT F - FEDERAL FUNDS CERTIFICATIONS

FEDERAL CERTIFICATIONS
ADDENDUM FOR AGREEMENT FUNDED BY U.S. FEDERAL GRANT

TO WHOM IT MAY CONCERN:

Participating Agencies may elect to use federal funds to purchase under the Master Agreement. This form should be completed and returned.

DEFINITIONS

Contract means a legal instrument by which a non-Federal entity purchases property or services needed to carry out the project or program under a Federal award. The term as used in this part does not include a legal instrument, even if the non-Federal entity considers it a contract, when the substance of the transaction meets the definition of a Federal award or subaward

Contractor means an entity that receives a contract as defined in Contract.

Cooperative agreement means a legal instrument of financial assistance between a Federal awarding agency or pass-through entity and a non-Federal entity that, consistent with 31 U.S.C. 6302-6305:

- (a) Is used to enter into a relationship the principal purpose of which is to transfer anything of value from the Federal awarding agency or pass-through entity to the non-Federal entity to carry out a public purpose authorized by a law of the United States (see 31 U.S.C. 6101(3)); and not to acquire property or services for the Federal government or pass-through entity's direct benefit or use;
- (b) Is distinguished from a grant in that it provides for substantial involvement between the Federal awarding agency or pass-through entity and the non-Federal entity in carrying out the activity contemplated by the Federal award.
- (c) The term does not include:
 - (1) A cooperative research and development agreement as defined in 15 U.S.C. 3710a; or
 - (2) An agreement that provides only:
 - (i) Direct United States Government cash assistance to an individual;
 - (ii) A subsidy;
 - (iii) A loan;
 - (iv) A loan guarantee; or
 - (v) Insurance.

Federal awarding agency means the Federal agency that provides a Federal award directly to a non-Federal entity

Federal award has the meaning, depending on the context, in either paragraph (a) or (b) of this section:

- (a)(1) The Federal financial assistance that a non-Federal entity receives directly from a Federal awarding agency or indirectly from a pass-through entity, as described in § 200.101 Applicability; or
- (2) The cost-reimbursement contract under the Federal Acquisition Regulations that a non-Federal entity receives directly from a Federal awarding agency or indirectly from a pass-through entity, as described in § 200.101 Applicability.
- (b) The instrument setting forth the terms and conditions. The instrument is the grant agreement, cooperative agreement, other agreement for assistance covered in paragraph (b) of § 200.40 Federal financial assistance, or the cost-reimbursement contract awarded under the Federal Acquisition Regulations.
- (c) Federal award does not include other contracts that a Federal agency uses to buy goods or services from a contractor or a contract to operate Federal government owned, contractor operated facilities (GOCOs).
- (d) See also definitions of Federal financial assistance, grant agreement, and cooperative agreement.

Non-Federal entity means a state, local government, Indian tribe, institution of higher education (IHE), or nonprofit organization that carries out a Federal award as a recipient or subrecipient.

Nonprofit organization means any corporation, trust, association, cooperative, or other organization, not including IHEs, that:

- (a) Is operated primarily for scientific, educational, service, charitable, or similar purposes in the public interest;
- (b) Is not organized primarily for profit; and

**OMNIA PARTNERS EXHIBITS
EXHIBIT F - FEDERAL FUNDS CERTIFICATIONS**

(c) Uses net proceeds to maintain, improve, or expand the operations of the organization.

Obligations means, when used in connection with a non-Federal entity's utilization of funds under a Federal award, orders placed for property and services, contracts and subawards made, and similar transactions during a given period that require payment by the non-Federal entity during the same or a future period.

Pass-through entity means a non-Federal entity that provides a subaward to a subrecipient to carry out part of a Federal program.

Recipient means a non-Federal entity that receives a Federal award directly from a Federal awarding agency to carry out an activity under a Federal program. The term recipient does not include subrecipients.

Simplified acquisition threshold means the dollar amount below which a non-Federal entity may purchase property or services using small purchase methods. Non-Federal entities adopt small purchase procedures in order to expedite the purchase of items costing less than the simplified acquisition threshold. The simplified acquisition threshold is set by the Federal Acquisition Regulation at 48 CFR Subpart 2.1 (Definitions) and in accordance with 41 U.S.C. 1908. As of the publication of this part, the simplified acquisition threshold is \$150,000, but this threshold is periodically adjusted for inflation. (Also see definition of § 200.67 Micro-purchase.)

Subaward means an award provided by a pass-through entity to a subrecipient for the subrecipient to carry out part of a Federal award received by the pass-through entity. It does not include payments to a contractor or payments to an individual that is a beneficiary of a Federal program. A subaward may be provided through any form of legal agreement, including an agreement that the pass-through entity considers a contract.

Subrecipient means a non-Federal entity that receives a subaward from a pass-through entity to carry out part of a Federal program; but does not include an individual that is a beneficiary of such program. A subrecipient may also be a recipient of other Federal awards directly from a Federal awarding agency.

Termination means the ending of a Federal award, in whole or in part at any time prior to the planned end of period of performance.

The following certifications and provisions may be required and apply when Participating Agency expends federal funds for any purchase resulting from this procurement process. Pursuant to 2 C.F.R. § 200.326, all contracts, including small purchases, awarded by the Participating Agency and the Participating Agency's subcontractors shall contain the procurement provisions of Appendix II to Part 200, as applicable.

APPENDIX II TO 2 CFR PART 200

(A) Contracts for more than the simplified acquisition threshold currently set at \$150,000, which is the inflation adjusted amount determined by the Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council (Councils) as authorized by 41 U.S.C. 1908, must address administrative, contractual, or legal remedies in instances where contractors violate or breach contract terms, and provide for such sanctions and penalties as appropriate.

Pursuant to Federal Rule (A) above, when a Participating Agency expends federal funds, the Participating Agency reserves all rights and privileges under the applicable laws and regulations with respect to this procurement in the event of breach of contract by either party.

Does offeror agree? YES  Initials of Authorized Representative of offeror

(B) Termination for cause and for convenience by the grantee or subgrantee including the manner by which it will be effected and the basis for settlement. (All contracts in excess of \$10,000)

Pursuant to Federal Rule (B) above, when a Participating Agency expends federal funds, the Participating Agency reserves the right to immediately terminate any agreement in excess of \$10,000 resulting from this procurement process in the event of a breach or default of the agreement by Offeror as detailed in the terms of the contract.

Does offeror agree? YES  Initials of Authorized Representative of offeror

Requirements for National Cooperative Contract

OMNIA PARTNERS EXHIBITS

EXHIBIT F - FEDERAL FUNDS CERTIFICATIONS

offeror

(C) Equal Employment Opportunity. Except as otherwise provided under 41 CFR Part 60, all contracts that meet the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3 must include the equal opportunity clause provided under 41 CFR 60-1.4(b), in accordance with Executive Order 11246, "Equal Employment Opportunity" (30 CFR 12319, 12935, 3 CFR Part, 1964-1965 Comp., p. 339), as amended by Executive Order 11375, "Amending Executive Order 11246 Relating to Equal Employment Opportunity," and implementing regulations at 41 CFR part 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor."

Pursuant to Federal Rule (C) above, when a Participating Agency expends federal funds on any federally assisted construction contract, the equal opportunity clause is incorporated by reference herein.

Does offeror agree to abide by the above? YES  Initials of Authorized Representative of offeror

(D) Davis-Bacon Act, as amended (40 U.S.C. 3141-3148). When required by Federal program legislation, all prime construction contracts in excess of \$2,000 awarded by non-Federal entities must include a provision for compliance with the Davis-Bacon Act (40 U.S.C. 3141-3144, and 3146-3148) as supplemented by Department of Labor regulations (29 CFR Part 5, "Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction"). In accordance with the statute, contractors must be required to pay wages to laborers and mechanics at a rate not less than the prevailing wages specified in a wage determination made by the Secretary of Labor. In addition, contractors must be required to pay wages not less than once a week. The non-Federal entity must place a copy of the current prevailing wage determination issued by the Department of Labor in each solicitation. The decision to award a contract or subcontract must be conditioned upon the acceptance of the wage determination. The non-Federal entity must report all suspected or reported violations to the Federal awarding agency. The contracts must also include a provision for compliance with the Copeland "Anti-Kickback" Act (40 U.S.C. 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, "Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States"). The Act provides that each contractor or subrecipient must be prohibited from inducing, by any means, any person employed in the construction, completion, or repair of public work, to give up any part of the compensation to which he or she is otherwise entitled. The non-Federal entity must report all suspected or reported violations to the Federal awarding agency.

Pursuant to Federal Rule (D) above, when a Participating Agency expends federal funds during the term of an award for all contracts and subgrants for construction or repair, offeror will be in compliance with all applicable Davis-Bacon Act provisions.

Does offeror agree? YES  Initials of Authorized Representative of offeror

(E) Contract Work Hours and Safety Standards Act (40 U.S.C. 3701-3708). Where applicable, all contracts awarded by the non-Federal entity in excess of \$100,000 that involve the employment of mechanics or laborers must include a provision for compliance with 40 U.S.C. 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5). Under 40 U.S.C. 3702 of the Act, each contractor must be required to compute the wages of every mechanic and laborer on the basis of a standard work week of 40 hours. Work in excess of the standard work week is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of 40 hours in the work week. The requirements of 40 U.S.C. 3704 are applicable to construction work and provide that no laborer or mechanic must be required to work in surroundings or under working conditions which are unsanitary, hazardous or dangerous. These requirements do not apply to the purchases of supplies or materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.

Pursuant to Federal Rule (E) above, when a Participating Agency expends federal funds, offeror certifies that offeror will be in compliance with all applicable provisions of the Contract Work Hours and Safety Standards Act during the term of an award for all contracts by Participating Agency resulting from this procurement process.

Does offeror agree? YES  Initials of Authorized Representative of offeror

(F) Rights to Inventions Made Under a Contract or Agreement. If the Federal award meets the definition of "funding agreement" under 37 CFR §401.2 (a) and the recipient or subrecipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance of experimental, developmental, or research work under that "funding agreement," the recipient or subrecipient must comply with the requirements of 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small

OMNIA PARTNERS EXHIBITS

EXHIBIT F - FEDERAL FUNDS CERTIFICATIONS

Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency.

Pursuant to Federal Rule (F) above, when federal funds are expended by Participating Agency, the offeror certifies that during the term of an award for all contracts by Participating Agency resulting from this procurement process, the offeror agrees to comply with all applicable requirements as referenced in Federal Rule (F) above.

Does offeror agree? YES  Initials of Authorized Representative of offeror

(G) Clean Air Act (42 U.S.C. 7401-7671q.) and the Federal Water Pollution Control Act (33 U.S.C. 1251-1387), as amended—Contracts and subgrants of amounts in excess of \$150,000 must contain a provision that requires the non-Federal award to agree to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401-7671q) and the Federal Water Pollution Control Act as amended (33 U.S.C. 1251- 1387). Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA)

Pursuant to Federal Rule (G) above, when federal funds are expended by Participating Agency, the offeror certifies that during the term of an award for all contracts by Participating Agency member resulting from this procurement process, the offeror agrees to comply with all applicable requirements as referenced in Federal Rule (G) above.

Does offeror agree? YES  Initials of Authorized Representative of offeror

(H) Debarment and Suspension (Executive Orders 12549 and 12689)—A contract award (see 2 CFR 180.220) must not be made to parties listed on the government wide exclusions in the System for Award Management (SAM), in accordance with the Executive Office of the President Office of Management and Budget (OMB) guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR part 1986 Comp., p. 189) and 12689 (3 CFR part 1989 Comp., p. 235), "Debarment and Suspension." SAM Exclusions contains the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549.

Pursuant to Federal Rule (H) above, when federal funds are expended by Participating Agency, the offeror certifies that during the term of an award for all contracts by Participating Agency resulting from this procurement process, the offeror certifies that neither it nor its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation by any federal department or agency. If at any time during the term of an award the offeror or its principals becomes debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation by any federal department or agency, the offeror will notify the Participating Agency.

Does offeror agree? YES  Initials of Authorized Representative of offeror

(I) Byrd Anti-Lobbying Amendment (31 U.S.C. 1352)—Contractors that apply or bid for an award exceeding \$100,000 must file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352. Each tier must also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the non-Federal award.

Pursuant to Federal Rule (I) above, when federal funds are expended by Participating Agency, the offeror certifies that during the term and after the awarded term of an award for all contracts by Participating Agency resulting from this procurement process, the offeror certifies that it is in compliance with all applicable provisions of the Byrd Anti-Lobbying Amendment (31 U.S.C. 1352). The undersigned further certifies that:

- (1) No Federal appropriated funds have been paid or will be paid for on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of congress, or an employee of a Member of Congress in connection with the awarding of a Federal contract, the making of a Federal grant, the making of a Federal loan, the entering into a cooperative agreement, and the extension, continuation, renewal, amendment, or modification of a Federal contract, grant, loan, or cooperative agreement.
- (2) If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of congress, or an employee of a Member of Congress in connection with this Federal grant or cooperative agreement, the undersigned shall

OMNIA PARTNERS EXHIBITS

EXHIBIT F - FEDERAL FUNDS CERTIFICATIONS

complete and submit Standard Form-LLL, "Disclosure Form to Report Lobbying", in accordance with its instructions.

(3) The undersigned shall require that the language of this certification be included in the award documents for all covered sub-awards exceeding \$100,000 in Federal funds at all appropriate tiers and that all subrecipients shall certify and disclose accordingly.

Does offeror agree? YES [Signature] Initials of Authorized Representative of offeror

RECORD RETENTION REQUIREMENTS FOR CONTRACTS INVOLVING FEDERAL FUNDS

When federal funds are expended by Participating Agency for any contract resulting from this procurement process, offeror certifies that it will comply with the record retention requirements detailed in 2 CFR § 200.333. The offeror further certifies that offeror will retain all records as required by 2 CFR § 200.333 for a period of three years after grantees or subgrantees submit final expenditure reports or quarterly or annual financial reports, as applicable, and all other pending matters are closed.

Does offeror agree? YES [Signature] Initials of Authorized Representative of offeror

CERTIFICATION OF COMPLIANCE WITH THE ENERGY POLICY AND CONSERVATION ACT

When Participating Agency expends federal funds for any contract resulting from this procurement process, offeror certifies that it will comply with the mandatory standards and policies relating to energy efficiency which are contained in the state energy conservation plan issued in compliance with the Energy Policy and Conservation Act (42 U.S.C. 6321 et seq.; 49 C.F.R. Part 18).

Does offeror agree? YES [Signature] Initials of Authorized Representative of offeror

CERTIFICATION OF COMPLIANCE WITH BUY AMERICA PROVISIONS

To the extent purchases are made with Federal Highway Administration, Federal Railroad Administration, or Federal Transit Administration funds, offeror certifies that its products comply with all applicable provisions of the Buy America Act and agrees to provide such certification or applicable waiver with respect to specific products to any Participating Agency upon request. Purchases made in accordance with the Buy America Act must still follow the applicable procurement rules calling for free and open competition.

Does offeror agree? YES [Signature] Initials of Authorized Representative of offeror

CERTIFICATION OF ACCESS TO RECORDS - 2 C.F.R. § 200.336

Offeror agrees that the Inspector General of the Agency or any of their duly authorized representatives shall have access to any documents, papers, or other records of offeror that are pertinent to offeror's discharge of its obligations under the Contract for the purpose of making audits, examinations, excerpts, and transcriptions. The right also includes timely and reasonable access to offeror's personnel for the purpose of interview and discussion relating to such documents.

Does offeror agree? YES [Signature] Initials of Authorized Representative of offeror

CERTIFICATION OF APPLICABILITY TO SUBCONTRACTORS

Offeror agrees that all contracts it awards pursuant to the Contract shall be bound by the foregoing terms and conditions.

Does offeror agree? YES [Signature] Initials of Authorized Representative of offeror

Offeror agrees to comply with all federal, state, and local laws, rules, regulations and ordinances, as applicable. It is further acknowledged that offeror certifies compliance with all provisions, laws, acts, regulations, etc. as specifically noted above.

Offeror's Name: Fischer International Identity, LLC

Address, City, State, and Zip Code: 9045 Strada Stell G., Ste 201, Naples FL 34110

OMNIA PARTNERS EXHIBITS
EXHIBIT F - FEDERAL FUNDS CERTIFICATIONS

Phone Number: 239-643-1500 Fax Number: _____

Printed Name and Title of Authorized Representative: R. Andrew SROKA, CEO

Email Address: Andrew.S@FischerIdentity.com

Signature of Authorized Representative:  Date: 10/16/2020

EXHIBIT G
NEW JERSEY BUSINESS COMPLIANCE

NEW JERSEY BUSINESS COMPLIANCE

Suppliers intending to do business in the State of New Jersey must comply with policies and procedures required under New Jersey statutes. All offerors submitting proposals must complete the following forms specific to the State of New Jersey. Completed forms should be submitted with the offeror's response to the RFP. Failure to complete the New Jersey packet will impact OMNIA Partners' ability to promote the Master Agreement in the State of New Jersey.

DOC #1	Ownership Disclosure Form
DOC #2	Non-Collusion Affidavit
DOC #3	Affirmative Action Affidavit
DOC #4	Political Contribution Disclosure Form
DOC #5	Stockholder Disclosure Certification
DOC #6	Certification of Non-Involvement in Prohibited Activities in Iran
DOC #7	New Jersey Business Registration Certificate
DOC #8	Equal Employment Opportunity/Affirmative Action Evidence
DOC #9	McBride Principles

New Jersey suppliers are required to comply with the following New Jersey statutes when applicable:

- all anti-discrimination laws, including those contained in N.J.S.A. 10:2-1 through N.J.S.A. 10:2-14, N.J.S.A. 10:5-1, and N.J.S.A. 10:5-31 through 10:5-38;
- Prevailing Wage Act, N.J.S.A. 34:11-56.26, for all contracts within the contemplation of the Act;
- Public Works Contractor Registration Act, N.J.S.A. 34:11-56.26; and
- Bid and Performance Security, as required by the applicable municipal or state statutes.

STATEMENT OF OWNERSHIP DISCLOSURE

N.J.S.A. 52:25-24.2 (P.L. 1977, c.33, as amended by P.L. 2016, c.43)

This statement shall be completed, certified to, and included with all bid and proposal submissions. Failure to submit the required information is cause for automatic rejection of the bid or proposal.

Name of Organization: Fischer International Identity, LLC

Organization Address: 9045 Strada Stell Ct., Suite 201, Naples, FL 34109

Part I Check the box that represents the type of business organization:

- Sole Proprietorship (skip Parts II and III, execute certification in Part IV)
- Non-Profit Corporation (skip Parts II and III, execute certification in Part IV)
- For-Profit Corporation (any type) Limited Liability Company (LLC)
- Partnership Limited Partnership Limited Liability Partnership (LLP)
- Other (be specific): _____

Part II

- The list below contains the names and addresses of all stockholders in the corporation who own 10 percent or more of its stock, of any class, or of all individual partners in the partnership who own a 10 percent or greater interest therein, or of all members in the limited liability company who own a 10 percent or greater interest therein, as the case may be. **(COMPLETE THE LIST BELOW IN THIS SECTION)**

OR

- No one stockholder in the corporation owns 10 percent or more of its stock, of any class, or no individual partner in the partnership owns a 10 percent or greater interest therein, or no member in the limited liability company owns a 10 percent or greater interest therein, as the case may be. **(SKIP TO PART IV)**

(Please attach additional sheets if more space is needed):

Name of Individual or Business Entity	Home Address (for Individuals) or Business Address
Addison M. Fischer, as Trustee of the Addison M. Fischer Revocable Trust created under declaration of trust dated April 13, 2016	5801 Pelican Bay Blvd., Suite 104, Naples, FL 34108

Part III DISCLOSURE OF 10% OR GREATER OWNERSHIP IN THE STOCKHOLDERS, PARTNERS OR LLC MEMBERS LISTED IN PART II

If a bidder has a direct or indirect parent entity which is publicly traded, and any person holds a 10 percent or greater beneficial interest in the publicly traded parent entity as of the last annual federal Security and Exchange Commission (SEC) or foreign equivalent filing, ownership disclosure can be met by providing links to the website(s) containing the last annual filing(s) with the federal Securities and Exchange Commission (or foreign equivalent) that contain the name and address of each person holding a 10% or greater beneficial interest in the publicly traded parent entity, along with the relevant page numbers of the filing(s) that contain the information on each such person. **Attach additional sheets if more space is needed.**

Website (URL) containing the last annual SEC (or foreign equivalent) filing	Page #'s
N/A	

Please list the names and addresses of each stockholder, partner or member owning a 10 percent or greater interest in any corresponding corporation, partnership and/or limited liability company (LLC) listed in Part II **other than for any publicly traded parent entities referenced above.** The disclosure shall be continued until names and addresses of every noncorporate stockholder, and individual partner, and member exceeding the 10 percent ownership criteria established pursuant to N.J.S.A. 52:25-24.2 has been listed. **Attach additional sheets if more space is needed.**

Stockholder/Partner/Member and Corresponding Entity Listed in Part II	Home Address (for Individuals) or Business Address
N/A	

Part IV Certification

I, being duly sworn upon my oath, hereby represent that the foregoing information and any attachments thereto to the best of my knowledge are true and complete. I acknowledge: that I am authorized to execute this certification on behalf of the bidder/proposer; that the **<name of contracting unit>** is relying on the information contained herein and that I am under a continuing obligation from the date of this certification through the completion of any contracts with **<type of contracting unit>** to notify the **<type of contracting unit>** in writing of any changes to the information contained herein; that I am aware that it is a criminal offense to make a false statement or misrepresentation in this certification, and if I do so, I am subject to criminal prosecution under the law and that it will constitute a material breach of my agreement(s) with the, permitting the **<type of contracting unit>** to declare any contract(s) resulting from this certification void and unenforceable.

Full Name (Print):	R. Andrew Sroka	Title:	President & CEO
Signature:		Date:	10/22/2020

DOC #2

NON-COLLUSION AFFIDAVIT

STANDARD BID DOCUMENT REFERENCE	
	Reference: VII-H
Name of Form:	NON-COLLUSION AFFIDAVIT
Statutory Reference:	No specific statutory reference State Statutory Reference N.J.S.A. 52:34-15
Instructions Reference:	Statutory and Other Requirements VII-H
Description:	The Owner's use of this form is optional. It is used to ensure that the bidder has not participated in any collusion with any other bidder or Owner representative or otherwise taken any action in restraint of free and competitive bidding.

NON-COLLUSION AFFIDAVIT

State of ~~New Jersey~~ Florida
County of Collier

ss:

I, R. Andrew Sroka residing in Naples
(name of affiant) (name of municipality)
in the County of Collier and State of Florida of full
age, being duly sworn according to law on my oath depose and say that:

I am President & CEO of the firm of Fischer International
(title or position) (name of firm)

Identity, LLC the bidder making this Proposal for the bid

entitled [REDACTED], and that I executed the said proposal with
(title of bid proposal)
full authority to do so that said bidder has not, directly or indirectly entered into any agreement,
participated in any collusion, or otherwise taken any action in restraint of free, competitive bidding in
connection with the above named project; and that all statements contained in said proposal and in this
affidavit are true and correct, and made with full knowledge that the [REDACTED]
(name of contracting unit) relies upon the truth of the statements contained in said Proposal
and in the statements contained in this affidavit in awarding the contract for the said project.

I further warrant that no person or selling agency has been employed or retained to solicit or secure such
contract upon an agreement or understanding for a commission, percentage, brokerage, or contingent
fee, except bona fide employees or bona fide established commercial or selling agencies maintained by
[REDACTED]

Subscribed and sworn to

before me this day



Signature

R. Andrew Sroka

(Type or print name of affiant under signature)

Oct. 22nd, 2020

[Handwritten Signature]
Notary public of

My Commission expires 8/21/22

(Seal)



KAYLA MARIE MCCANS
Commission # GG 250428
Expires August 21, 2022
Bonded Thru Budget Notary Services

DOC #3

**AFFIRMATIVE ACTION AFFIDAVIT
(P.L. 1975, C.127)**

Company Name: Fischer International Identity, LLC
Street: 9045 Strada Stell Ct., Suite 201
City, State, Zip Code: Naples, FL 34109

Proposal Certification:

Indicate below company's compliance with New Jersey Affirmative Action regulations. Company's proposal will be accepted even if company is not in compliance at this time. No contract and/or purchase order may be issued, however, until all Affirmative Action requirements are met.

Required Affirmative Action Evidence:

Procurement, Professional & Service Contracts (Exhibit A)

Vendors must submit with proposal:

1. A photo copy of their Federal Letter of Affirmative Action Plan Approval

OR
2. A photo copy of their Certificate of Employee Information Report

OR
3. A complete Affirmative Action Employee Information Report (AA302) _____

Public Work – Over \$50,000 Total Project Cost:

- A. No approved Federal or New Jersey Affirmative Action Plan. We will complete Report Form AA201-A upon receipt from the
- B. Approved Federal or New Jersey Plan – certificate enclosed

I further certify that the statements and information contained herein, are complete and correct to the best of my knowledge and belief.

10/22/2020
Date


Authorized Signature and Title

DOC #3, continued

P.L. 1995, c. 127 (N.J.A.C. 17:27)
MANDATORY AFFIRMATIVE ACTION LANGUAGE

PROCUREMENT, PROFESSIONAL AND SERVICE
CONTRACTS

During the performance of this contract, the contractor agrees as follows:

The contractor or subcontractor, where applicable, will not discriminate against any employee or applicant for employment because of age, race, creed, color, national origin, ancestry, marital status, sex, affectional or sexual orientation. The contractor will take affirmative action to ensure that such applicants are recruited and employed, and that employees are treated during employment, without regard to their age, race, creed, color, national origin, ancestry, marital status, sex, affectional or sexual orientation. Such action shall include, but not be limited to the following: employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. The contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided by the Public Agency Compliance Officer setting forth provisions of this non-discrimination clause.

The contractor or subcontractor, where applicable will, in all solicitations or advertisement for employees placed by or on behalf of the contractor, state that all qualified applicants will receive consideration for employment without regard to age, race, creed, color, national origin, ancestry, marital status, sex, affectional or sexual orientation.

The contractor or subcontractor, where applicable, will send to each labor union or representative of workers with which it has a collective bargaining agreement or other contract or understanding, a notice, to be provided by the agency contracting officer advising the labor union or workers' representative of the contractor's commitments under this act and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

The contractor or subcontractor, where applicable, agrees to comply with any regulations promulgated by the Treasurer pursuant to P.L. 1975, c. 127, as amended and supplemented from time to time and the Americans with Disabilities Act.

The contractor or subcontractor agrees to attempt in good faith to employ minority and female workers trade consistent with the applicable county employment goal prescribed by N.J.A.C. 17:27-5.2 promulgated by the Treasurer pursuant to P.L. 1975, C.127, as amended and supplemented from time to time or in accordance with a binding determination of the applicable county employment goals determined by the Affirmative Action Office pursuant to N.J.A.C. 17:27-5.2 promulgated by the Treasurer pursuant to P.L. 1975, C.127, as amended and supplemented from time to time.

The contractor or subcontractor agrees to inform in writing appropriate recruitment agencies in the area, including employment agencies, placement bureaus, colleges, universities, labor unions, that it does not discriminate on the basis of age, creed, color, national origin, ancestry, marital status, sex, affectional or sexual orientation, and that it will discontinue the use of any recruitment agency which engages in direct or indirect discriminatory practices.

The contractor or subcontractor agrees to revise any of its testing procedures, if necessary, to assure that all personnel testing conforms with the principles of job-related testing, as established by the statutes and court decisions of the state of New Jersey and as established by applicable Federal law and applicable Federal court decisions.

The contractor or subcontractor agrees to review all procedures relating to transfer, upgrading, downgrading and lay-off to ensure that all such actions are taken without regard to age, creed, color, national origin, ancestry, marital status, sex, affectional or sexual orientation, and conform with the applicable employment goals, consistent with the statutes and court decisions of the State of New Jersey, and applicable Federal law and applicable Federal court decisions.

The contractor and its subcontractors shall furnish such reports or other documents to the Affirmative Action Office as may be requested by the office from time to time in order to carry out the purposes of these regulations, and public agencies shall furnish such information as may be requested by the Affirmative Action Office for conducting a compliance investigation pursuant to Subchapter 10 of the Administrative Code (NJAC 17:27).


Signature of Procurement Agent

C. 271 POLITICAL CONTRIBUTION DISCLOSURE FORM

Public Agency Instructions

This page provides guidance to public agencies entering into contracts with business entities that are required to file Political Contribution Disclosure forms with the agency. **It is not intended to be provided to contractors.** What follows are instructions on the use of form local units can provide to contractors that are required to disclose political contributions pursuant to N.J.S.A. 19:44A-20.26 (P.L. 2005, c. 271, s.2). Additional information on the process is available in Local Finance Notice 2006-1 (http://www.nj.gov/dca/divisions/dlgs/resources/lfns_2006.html). Please refer back to these instructions for the appropriate links, as the Local Finance Notices include links that are no longer operational.

1. The disclosure is required for all contracts in excess of \$17,500 that are **not awarded** pursuant to a “fair and open” process (N.J.S.A. 19:44A-20.7).
2. Due to the potential length of some contractor submissions, the public agency should consider allowing data to be submitted in electronic form (i.e., spreadsheet, pdf file, etc.). Submissions must be kept with the contract documents or in an appropriate computer file and be available for public access. **The form is worded to accept this alternate submission.** The text should be amended if electronic submission will not be allowed.
3. The submission must be **received from the contractor and** on file at least 10 days prior to award of the contract. Resolutions of award should reflect that the disclosure has been received and is on file.
4. The contractor must disclose contributions made to candidate and party committees covering a wide range of public agencies, including all public agencies that have elected officials in the county of the public agency, state legislative positions, and various state entities. The Division of Local Government Services recommends that contractors be provided a list of the affected agencies. This will assist contractors in determining the campaign and political committees of the officials and candidates affected by the disclosure.
 - a. The Division has prepared model disclosure forms for each county. They can be downloaded from the “County PCD Forms” link on the Pay-to-Play web site at <http://www.nj.gov/dca/divisions/dlgs/programs/lpcl.html#12>. They will be updated from time-to-time as necessary.
 - b. A public agency using these forms should **edit them to properly reflect the correct legislative district(s)**. As the forms are county-based, **they list all legislative districts in each county. Districts that do not represent the public agency should be removed from the lists.**
 - c. Some contractors may find it easier to provide a single list that covers all contributions, regardless of the county. These submissions are appropriate and should be accepted.
 - d. The form may be used “as-is”, subject to edits as described herein.
 - e. The “Contractor Instructions” sheet is intended to be provided with the form. It is recommended that the Instructions and the form be printed on the same piece of paper. The form notes that the Instructions are printed on the back of the form; where that is not the case, the text should be edited accordingly.
 - f. The form is a Word document and can be edited to meet local needs, and posted for download on web sites, used as an e-mail attachment, or provided as a printed document.
5. It is recommended that the contractor also complete a “Stockholder Disclosure Certification.” This will assist the local unit in its obligation to ensure that contractor did not make any prohibited contributions to the committees listed on the Business Entity Disclosure Certification in the 12 months prior to the contract (See Local Finance Notice 2006-7 for additional information on this obligation at http://www.nj.gov/dca/divisions/dlgs/resources/lfns_2006.html). A sample Certification form is part of this package and the instruction to complete it is included in the Contractor Instructions. NOTE: This section is not applicable to Boards of Education.

C. 271 POLITICAL CONTRIBUTION DISCLOSURE FORM

Contractor Instructions

Business entities (contractors) receiving contracts from a public agency that are NOT awarded pursuant to a “fair and open” process (defined at N.J.S.A. 19:44A-20.7) are subject to the provisions of P.L. 2005, c. 271, s.2 (N.J.S.A. 19:44A-20.26). This law provides that 10 days prior to the award of such a contract, the contractor shall disclose contributions to:

- any State, county, or municipal committee of a political party
- any legislative leadership committee*
- any continuing political committee (a.k.a., political action committee)
- any candidate committee of a candidate for, or holder of, an elective office:
 - of the public entity awarding the contract
 - of that county in which that public entity is located
 - of another public entity within that county
 - or of a legislative district in which that public entity is located or, when the public entity is a county, of any legislative district which includes all or part of the county

The disclosure must list reportable contributions to any of the committees that exceed \$300 per election cycle that were made during the 12 months prior to award of the contract. See N.J.S.A. 19:44A-8 and 19:44A-16 for more details on reportable contributions.

N.J.S.A. 19:44A-20.26 itemizes the parties from whom contributions must be disclosed when a business entity is not a natural person. This includes the following:

- individuals with an “interest” ownership or control of more than 10% of the profits or assets of a business entity or 10% of the stock in the case of a business entity that is a corporation for profit
- all principals, partners, officers, or directors of the business entity or their spouses
- any subsidiaries directly or indirectly controlled by the business entity
- IRS Code Section 527 New Jersey based organizations, directly or indirectly controlled by the business entity and filing as continuing political committees, (PACs).

When the business entity is a natural person, “a contribution by that person’s spouse or child, residing therewith, shall be deemed to be a contribution by the business entity.” [N.J.S.A. 19:44A-20.26(b)] The contributor must be listed on the disclosure.

Any business entity that fails to comply with the disclosure provisions shall be subject to a fine imposed by ELEC in an amount to be determined by the Commission which may be based upon the amount that the business entity failed to report.

The enclosed list of agencies is provided to assist the contractor in identifying those public agencies whose elected official and/or candidate campaign committees are affected by the disclosure requirement. It is the contractor’s responsibility to identify the specific committees to which contributions may have been made and need to be disclosed. The disclosed information may exceed the minimum requirement.

The enclosed form, a content-consistent facsimile, or an electronic data file containing the required details (along with a signed cover sheet) may be used as the contractor’s submission and is disclosable to the public under the Open Public Records Act.

The contractor must also complete the attached Stockholder Disclosure Certification. This will assist the agency in meeting its obligations under the law. **NOTE: This section does not apply to Board of Education contracts.**

* N.J.S.A. 19:44A-3(s): “The term “legislative leadership committee” means a committee established, authorized to be established, or designated by the President of the Senate, the Minority Leader of the Senate, the Speaker of the General Assembly or the Minority Leader of the General Assembly pursuant to section 16 of P.L.1993, c.65 (C.19:44A-10.1) for the purpose of receiving contributions and making expenditures.”

DOC #4, continued

List of Agencies with Elected Officials Required for Political Contribution Disclosure
N.J.S.A. 19:44A-20.26

County Name:

State: Governor, and Legislative Leadership Committees

Legislative District #s:

State Senator and two members of the General Assembly per district.

County:

Freeholders

{County Executive}

County Clerk

Surrogate

Sheriff

Municipalities (Mayor and members of governing body, regardless of title):

**USERS SHOULD CREATE THEIR OWN FORM, OR DOWNLOAD
FROM THE PAY TO PLAY SECTION OF THE DLGS WEBSITE A
COUNTY-BASED, CUSTOMIZABLE FORM.**

STOCKHOLDER DISCLOSURE CERTIFICATION

Name of Business:

I certify that the list below contains the names and home addresses of all stockholders holding 10% or more of the issued and outstanding stock of the undersigned.

OR

I certify that no one stockholder owns 10% or more of the issued and outstanding stock of the undersigned.

Check the box that represents the type of business organization:

Partnership

Corporation

Sole Proprietorship

Limited Partnership

Limited Liability Corporation

Limited Liability Partnership


Subchapter S Corporation

Sign and notarize the form below, and, if necessary, complete the stockholder list below.


Stockholders:

Name: Addison M. Fischer, as Trustee of the Addison M. Fischer Revocable Trust created under declaration of trust dated April 13, 2016	Name:
Home Address: 5801 Pelican Bay Blvd., #104, Naples, FL 34108	Home Address:
Name:	Name:
Home Address:	Home Address:
Name:	Name:
Home Address:	Home Address:

Subscribed and sworn before me this 22nd day of Oct, 2020

(Notary Public) 

My Commission expires: 8/21/22


(Affiant)
R. Andrew Sroka, President & CEO
(Print name & title of affiant)
(Corporate Seal)



DOC #6

Certification of Non-Involvement in Prohibited Activities in Iran

Pursuant to N.J.S.A. 52:32-58, Offerors must certify that neither the Offeror, nor any of its parents, subsidiaries, and/or affiliates (as defined in N.J.S.A. 52:32 – 56(e) (3)), is listed on the Department of the Treasury’s List of Persons or Entities Engaging in Prohibited Investment Activities in Iran and that neither is involved in any of the investment activities set forth in N.J.S.A. 52:32 – 56(f).

Offerors wishing to do business in New Jersey through this contract must fill out the Certification of Non-Involvement in Prohibited Activities in Iran here:

http://www.state.nj.us/humanservices/dfd/info/standard/fdc/disclosure_investmentact.pdf.

Offerors should submit the above form completed with their proposal.

DOC #7

**NEW JERSEY BUSINESS REGISTRATION CERTIFICATE
(N.J.S.A. 52:32-44)**

Offerors wishing to do business in New Jersey must submit their State Division of Revenue issued Business Registration Certificate with their proposal here. Failure to do so will disqualify the Offeror from offering products or services in New Jersey through any resulting contract.

<https://www.njportal.com/DOR/BusinessRegistration/>

DOC #8

EEOAA EVIDENCE

Equal Employment Opportunity/Affirmative Action
Goods, Professional Services & General Service Projects

EEO/AA Evidence

Vendors are required to submit evidence of compliance with N.J.S.A. 10:5-31 et seq. and N.J.A.C. 17:27 in order to be considered a responsible vendor.

One of the following must be included with submission:

- Copy of Letter of Federal Approval
- Certificate of Employee Information Report
- Fully Executed Form AA302
- Fully Executed EEO-1 Report

See the guidelines at: http://www.state.nj.us/treasury/contract_compliance/pdf/pa.pdf for further information.

I certify that my bid package includes the required evidence per the above list and State website.

Name: R. Andrew Sroka Title: President & CEO

Signature:  Date: 10/22/2020

DOC #9
MCBRIDE-PRINCIPLES



STATE OF NEW JERSEY DEPARTMENT OF THE TREASURY
DIVISION OF PURCHASE AND PROPERTY

33 WEST STATE STREET, P.O. BOX 230
TRENTON, NEW JERSEY 08625-0230

MACBRIDE PRINCIPALS FORM

BID SOLICITATION #: _____

VENDOR/BIDDER: _____

**VENDOR'S/BIDDER'S REQUIREMENT
TO PROVIDE A CERTIFICATION IN COMPLIANCE WITH THE MACBRIDE PRINCIPALS
AND NORTHERN IRELAND ACT OF 1989**

Pursuant to Public Law 1995, c. 134, a responsible Vendor/Bidder selected, after public bidding, by the Director of the Division of Purchase and Property, pursuant to N.J.S.A. 52:34-12, must complete the certification below by checking one of the two options listed below and signing where indicated. If a Vendor/Bidder that would otherwise be awarded a purchase, contract or agreement does not complete the certification, then the Director may determine, in accordance with applicable law and rules, that it is in the best interest of the State to award the purchase, contract or agreement to another Vendor/Bidder that has completed the certification and has submitted a bid within five (5) percent of the most advantageous bid. If the Director finds contractors to be in violation of the principals that are the subject of this law, he/she shall take such action as may be appropriate and provided by law, rule or contract, including but not limited to, imposing sanctions, seeking compliance, recovering damages, declaring the party in default and seeking debarment or suspension of the party.

I, the undersigned, on behalf the Vendor/Bidder, certify pursuant to N.J.S.A. 52:34-12.2 that:

CHECK THE APPROPRIATE BOX

The Vendor/Bidder has no business operations in Northern Ireland; or

OR
The Vendor/Bidder will take lawful steps in good faith to conduct any business operations it has in Northern Ireland in accordance with the MacBride principals of nondiscrimination in employment as set forth in section 2 of P.L. 1987, c. 177 (N.J.S.A. 52:18A-89.5) and in conformance with the United Kingdom's Fair Employment (Northern Ireland) Act of 1989, and permit independent monitoring of its compliance with those principals.

CERTIFICATION

I, the undersigned, certify that I am authorized to execute this certification on behalf of the Vendor/Bidder, that the foregoing information and any attachments hereto, to the best of my knowledge are true and complete. I acknowledge that the State of New Jersey is relying on the information contained herein, and that the Vendor/Bidder is under a continuing obligation from the date of this certification through the completion of any contract(s) with the State to notify the State in writing of any changes to the information contained herein; that I am aware that it is a criminal offense to make a false statement or misrepresentation in this certification. If I do so, I will be subject to criminal prosecution under the law, and it will constitute a material breach of my agreement(s) with the State, permitting the State to declare any contract(s) resulting from this certification to be void and unenforceable.

Signature

Date

Print Name and Title

STATE OF NEW JERSEY
BUSINESS REGISTRATION CERTIFICATE

DEPARTMENT OF TREASURY/
DIVISION OF REVENUE
PO BOX 252
TRENTON, N J 08646-0252

TAXPAYER NAME:
FISCHER INTERNATIONAL IDENTITY, LLC

TRADE NAME:

ADDRESS:
9045 STRADA STELL CT STE 201
NAPLES FL 34109-4438

SEQUENCE NUMBER:
2216405

EFFECTIVE DATE:

ISSUANCE DATE:

03/15/18

03/15/18



Director
New Jersey Division of Revenue

FORM 200

State of New Jersey - NOT A CONTRACT - This document is a record of the information provided by the taxpayer and is not a contract. It is subject to change without notice and is not a contract.