Request for Quote (RFQ)
Independent Identity Management (IdM) system

Summary
Society for Neuroscience (SfN) is seeking to transition from an Association Management System (AMS) Single Sign-On login (currently Personify) to one that is managed through an Independent Identity Management (IdM) system. We are looking to discuss your system's capabilities and how it can meet our organizational needs. We are looking for a demo to help us narrow down possible products and would like a tentative implementation timeline. The ultimate goal of this discovery process is to get a quote and select an appropriate system.

About Society for Neuroscience
The Society for Neuroscience (SfN) is the world's largest organization of scientists and physicians devoted to advancing the understanding of the brain and nervous system. SfN promotes scientific exchange through its annual meeting, which attracts more than 30,000 attendees from around the globe, and *The Journal of Neuroscience*, the field's most-cited peer-reviewed journal. SfN also supports the neuroscience community through professional development programming and is dedicated to sharing the excitement and progress of scientific discovery through public information and outreach. SfN advocates strongly for policies that advance science and improve health, such as robust federal research investments and the responsible use of animals in research.

Key Dates

Activity	Date
RFQ Release Date	August 28, 2017
Vendors to Submit Questions / RFQ Clarifications	August 28 – September 12, 2017
RFQ Response Deadline	September 20, 2017
Vendor Demo's	September 25 – October 20, 2017

Scope of Work

The selected system must meet the following organizational strategic imperatives:

1. SECURITY
    a. Enhance internal controls, provisioning, security, and compliance
    b. Ensure user access only to the data and applications that customers need (and are authorized)
    c. Respond to security issues quickly and proactively, increasing operational efficiency and internal controls
    d. Establish security processes to enable advanced two-factor user authentication

2. INTEGRATIONS
    a. Enable SSO across existing systems
    b. Assure that the selected IdM solution's SSO can be rebuilt to connect to any AMS

c. Anticipate future organizational needs to ensure that the system is able to mature with the industry and successfully integrate with new and emerging technologies

3. USER EXPERIENCE
    a. Support logins and provide improved user-experience for our customers across multiple sites and platforms
    b. Provide friendly user-interface of workflows for network connectivity and mobile access
    c. Balance privacy and security with ease-of-use

4. DATA HYGIENE
    a. Support organizational logins and access to manage information
    b. Reduce duplicates, to ensure data quality and integrity

Understanding of IdM System Capabilities

To help SfN understand the capabilities of your IdM solution, we have developed a series of questions that will allow us to better familiarize us with your specific solution and help guide the discussion. Please review each question and check the box, if your system has this capability. If not, please explain why. *Clarify / expand where needed.*

Please return this to us with a tentative implementation timeline and your availability for the initial discussion / presentation.

☐ Does the solution integrate with the Lightweight Directory Access Protocol, Microsoft Active Directory, or other common directory protocols?

☐ Does the IdM solution allow you to set policies for password difficulty and expiration?

☐ Can you specify minimum character ranges for passwords?

☐ Does the system log failed log-ins and allow you to lock out users after a specified number of failures?

☐ Does the solution support password encryption?

☐ Are passwords encrypted during both transmission and storage?

☐ What forms of encryption does the software support?

☐ Is there a self-provisioning module?

☐ Does it allow for automated retrieval of lost passwords?

☐ Does the IdM system provide different degrees of vetting for ID authentication, based on security clearance?

☐ Does it easily integrate with tokens, smart cards or other types of physical or biometric authentication?

☐ Will it support central caching of keys?

☐ Can it require different authentication criteria based on different trust levels?

☐ Can the solution be expanded to include new forms of identity verification and assertion, should they arise?

☐ Will the solution require users to periodically recertify their identities?

☐ Will it automatically propagate authorized changes across all system resources?

☐ Can it automatically locate and retire orphan accounts that are no longer in active use?

☐ How many roles does it allow you to create?

☐ How customizable are the rules for each role?

☐ Does the suite provide pre-built interfaces into core enterprise applications?

☐ Does it provide tools for customizing pre-built interfaces or building new ones from scratch?

☐ What kind of audit trail and reporting capabilities does the solution provide?

☐ Are the audit trails stored in a separate encrypted database?

☐ Can users create custom audit reports?

☐ Does the software support third-party audit tools?

☐ Does the solution allow for secure, offsite backup and restoration of identity data stores?

☐ What kind of service level agreements does the vendor provide?

☐ Does it offer 24/7 support or guaranteed minimum response times if its products fail?

Additional Information

Audience

At this time, we are only concerned with implementing IdM for our front-facing accounts (for our internal staff we use Active Directory). SfN has approximately 40,000 – 60,000 unique users logging into our SSOs annually. We have identified three groups as our audience:
(1) Individual SfN Members; (2) Company / Organization Level Accounts; and (3) External users of our websites (5 Web properties).

Assumptions

- SfN will be granted access to the Admin interface for authorization customizing
- Integration with on-premise and off-premise applications
- SfN will consider proposals of all hosting models
- Selected solution will be a strong enabler of mobile computing and will serve as a foundational component in mobile computing security
- The selected IdM Vendor has experience successfully implementing the tool for similar organizations

Project Timeline Targets – Phase 1

- Abstracts (CTI) SSO must be completed (or at least testable) by early March, 2018 prior to abstracts opening in April, 2018
- Registration (CDS) SSO must be completed (or at least testable) by early May, 2018 prior to registrations opening in June, 2018
- Scarce staff resources during the months of October and November, 2017 (due to our Annual Meeting) and December (due to holidays)
- Project Timelines will be based on a successful RFQ process and the selected vendor's availability / proposed schedule

---

Supplier Questions

Questions may be e-mailed to SfN Procurement Manager Egle Derkintyte: ederkintyte@sfn.org. Written questions should be directly tied to the RFQ by the supplier. Questions should be asked in constructive order, from beginning to end, following the organization of the RFQ. Each question should begin by referencing the RFQ page and section number to which it relates.

Submission

Interested candidates should provide a proposal to ederkintyte@sfn.org by 5 pm EDT September 20, 2017.

General Information

- Neither SfN nor its representatives shall be liable for any expenses a bidder incurs in connection with preparation of a response to this RFQ. Applicants should prepare their proposals simply and economically, providing a straightforward and concise description of the bidder's ability to meet the requirements of this RFQ.
- The issuance of this RFQ does not commit SfN to award a contract, to pay any costs incurred in the preparation of a proposal in response to this request or to actually procure the requested services.
- Gratuity Prohibition: Vendors shall not offer any gratuities, favors, or anything of monetary value to any associate at SfN for the purpose of influencing consideration of this proposal. If a SfN associate solicits a gratuity, the vendor is obligated to inform SfN's Deputy Executive Director.