

Office of Idaho State Controller

Brandon Woolf

Security Access Request

A Business Case for Updating the Security

Form Process to Enhance Application Security,

Improve Transparency, and Empower

State Agencies to Manage Staff-Level

Access to SCO Applications

Contents

[Background and Executive Summary 3](#_Toc481586308)

[How it Works 3](#_Toc481586309)

[Key Benefits 4](#_Toc481586310)

[Training 4](#_Toc481586311)

[Key Contact 5](#_Toc481586313)

# Background and Executive Summary

In preparation of modernizing Idaho’s core accounting and payroll systems, State Controller Brandon Woolf directed his staff to review all processes, functions and systems and to make recommendations regarding prioritizing work on pre-modernization projects.

At the State Controller’s direction and with an understanding of the security credentialing needs of state agencies, his staff developed a web-based solution to address and mitigate the inherent weaknesses in the legacy paper-based security form process. This new solution will be used by:

1. State agencies to communicate and approve their security needs to the State Controller’s Office; and
2. The State Controller’s Office to manage the underlying security data and workflows associated with granting, removing and modifying security privileges for accessing SCO applications.

# How it Works

The State Controller’s new web-based Security Access Request process works like many of the office’s other applications – authorized state agency users will access the new online Security Form by logging into the Application Selection page on the State Controller’s website. After logging into the Security Access Request, state agency users will be able to submit their requested security needs for a given user with one convenient paper-free online form. The request form will be automatically routed to the correct fulfillment teams at the SCO for rapid processing and turnaround.

This new process relies upon role-based workflows to communicate with approvers at the agency level via email to authorize security requests and changes, and to route the requests through the SCO’s security fulfillment teams for implementation. This step provides internal controls, further enhancing security while also improving accuracy.

Moreover, the new process allows state agencies to visually confirm who in their organization has access to which applications. This level of transparency was absent in the legacy manual process and will help ensure that only those with authority from their respective agency head have access to the applications. Moving to this new process will not only preserve the authorizations provided to agency staff, but it will also provide visibility to state agencies and empower them to manage the security access granted to their employees. The new web-based Security Access Request process will require little effort on the part of state agencies, other than participating in conveniently offered training.

From the standpoint of operational efficiency, the new Security Form process will allow SCO staff to manage workflows more effectively by providing certainty that a given request is processed in a timely manner by the appropriate fulfillment teams. Requests from agencies will travel through a single conduit for quicker response.

Because overall application security is highly dependent upon the accuracy of security credentialing, the new Security Access Request Form process improves accuracy by consolidating each user’s security provisions into individual, discrete records. This reduces the time and effort required to determine the exact resources any user may access. The role-based workflows behind the new Security Access Request process also provides a robust audit trail which further enhances accuracy.

# Benefits

* State agencies can now easily review who in their organization has access to which applications, empowering them to manage security credentials.
* The effort required by state agencies to utilize the new web-based Security Form process is minimal as current security authorizations are pre-loaded into the new process.
* The new, automated process reduces human errors and the possibility for miscommunication inherent in the legacy security credentialing process.
* The accuracy of security credentialing is improved by storing each user’s security access information in single, unique records.
* State agencies have a single point-of-entry for initiating security changes for all SCO applications and requests are promptly routed to the right SCO fulfillment team.
* Miscommunications between state agencies and SCO security fulfillment teams are dramatically reduced by standardizing the security process.
* The role-based workflows of the new Security Form process clearly articulates by whose authority changes may be requested and implemented while providing a robust audit trail which further ensures the integrity of security credentials.

# Training

Although the new Security Access Request process was designed to be intuitive and simple to use, SCO staff will be able to deliver training to state agency managers, payroll and fiscal staff through a variety of mediums which meet the agencies’ needs. Training seminars, which are open for both in-person and web-based participation are being scheduled, concise written training materials will be provided, and convenient and brief training videos are available.

Additionally, SCO help desk staff are prepared to help answer any questions you have and provide any assistance you may need using the new Security Access Request Form process via live telephone support and through email.

# Key Contact

For questions about the new Security Access Request process, training, or support, please contact the Office of the State Controller by calling (208) 334-3100 or via email to AccessRequest@sco.idaho.gov.