

Access Controls over the Business Services Online

A-03-13-13015



June 2014

Office of Audit Report Summary

Objective

To determine whether access controls for the Business Services Online (BSO) protected the Social Security Administration's (SSA) data and systems from misuse.

Background

As part of the employer suite of services, BSO enables users to electronically submit Wage and Tax Statements (Form W-2) to the Agency and verify the names and Social Security numbers (SSN) included on the wage reports via the Social Security Number Verification Service (SSNVS). In addition, BSO offers other suites of services including SSA services for Attorneys, Internet Representative Payee, and the Consent Based Social Security Number Verification service. For this review, we focused on wage reporting and SSNVS.

To access the BSO suite of services, users can register by telephone or the Internet using the Integrated Registration Services (IRES) application. IRES is a BSO sub-system that processes all registration and authentication requests. IRES allows users to register for a user identification and password and request access to applications in the BSO suite of services.

Our Findings

SSA's authentication, authorization, and monitoring controls needed strengthening to prevent and reduce the risk of unauthorized use of BSO services. Based on our sample of 1,673 registered users, we believe SSA erroneously authenticated and authorized 689 users and provided them access to BSO services.

The Agency authenticated six individuals and granted them access to BSO services when their personal information did not match SSA's Numident. Further, SSA granted the remaining 683 users access to BSO services; however, we found (1) 579 were children who were erroneously registered for employer-related services; (2) 80 were granted access even though there was no evidence these individuals worked for the companies they claimed to represent; and (3) 24 indicated they were self-employed, but none had self-employment income. In addition, 6 users who were not in our sample used BSO to submit 119 W-2s totaling \$188 million in fictitious wages. None of the six users worked for the companies they claimed to represent. Primarily, the users were granted access because SSA's age restriction control for children was not working as intended, and the Agency did not verify the employer-employee relationship until at least 1 year after access is granted.

SSA's maximum age check of 125-years-old did not effectively prevent unauthorized use of BSO services. We could not locate any verifiable records of individuals living to be age 125. We believe SSA should lower the maximum age check so the control could be more effective. In addition, SSA's control for monitoring registered users was not working as intended. SSA failed to deactivate the accounts of 212 users who died after they registered for BSO services. Finally, SSA did not have controls in place to ensure its employees and contractors were properly authorized to use BSO services. We found that 20 current or former SSA employees or contractors were registered BSO users but did not have a valid business reason to use the services.

Our Recommendations

We made a number of recommendations related to granting users access, ensuring users' access should remain active, age restriction controls, and deactivating users' accounts. SSA agreed with our recommendations.