The Background Screening Credentialing Council

The Background Screening Credentialing Council volunteer members drafted the following response to a question about Section 5 and Clause 1.1 of the BSAAP Standard, version 2.0, effective April 6, 2018. This letter is an informal discussion of the question posed and does not constitute a legal opinion of the BSCC.

TITLE: Section 5 – Verification Services Standards and Clause 1.1

Question: I am writing from my company, who submitted a Letter of Intent to apply for accreditation by December. I have two questions as I am working through preparing materials:

1. Would section 5 apply to my company if we aren't completing verifications ourselves but rather housing a database that reports verifications of employment regarding termination records between employers?

2. In regards to a security audit, would our company be able to submit application during a SOC2 Type 1 report before a SOC2 Type 2 audit and report is complete?

Response: In response to inquiry (1) above, Yes, "Section 5 Verification Services Standards" will still apply to your organization regardless of what source(s) of data you are utilizing to complete verification requests for your clients. This section (5) of the Standard addresses verification accuracy, having proper authorizations from consumers, communicating whether the original education data source is accredited or an otherwise recognized institution of higher education and learning, full disclosure to clients about general business practices, and procedures to ensure databases are managed properly to ensure maximum possible accuracy. If you believe there are certain clauses that are not applicable you may note the same within your submission, including an explanation as to why you believe the clause does not apply.

In response to inquiry (2) above, a submission which includes evidence of completion of a SOC2 Type 1 audit would not be acceptable as it does not meet the requirements of Clause 1.1.

Part of Clause 1.1 requires the CRA provide "written evidence of completing an information security audit for which no critical, high-risk, or severe security vulnerabilities remain uncured." A SOC2 Type 1 audit tests for the presence of written security controls and the appropriateness of those controls. In contrast, a SOC2 Type 2 audit (which includes SOC2 Type I requirements) tests to determine whether those controls are actually in place, being followed in the auditee's environment, and the effectiveness of those controls.

Because Clause 1.1 requires auditing of the actual use and effectiveness of security controls, a review and assessment of security documentation (as required by SOC2 Type 1) would not be sufficient to meet clause requirements.

We hope this response to your inquiries helps you as you prepare for the next step in the Accreditation process.

We believe we have responded fully to your inquiry. Please let us know if you have any further questions.