The Background Screening Credentialing Council has drafted the following response to a question we have received regarding the US Employment Screening / General Background Screening BSOAP Standard, this letter applies to US Version 2.0, 3.0 and General Version 1.0. This response is provided for *educational purposes only* and does not constitute legal advice, express or implied, of the BSCC, or the Professional Background Screening Association. Consultation with legal counsel is recommended in all matters of employment law.

For the purposes of this Letter, and to ensure our response applies to both Standards, the terms Organization and CRA may both be used.

TITLE: Clause 4.1 Public Record Researcher Agreement / 4.5 – Information Security

Issue (revised slightly): We have a client (an applicant Organization / CRA) that recently went through an audit. The auditor has told our client they need to call out '[insert platform provider]' as a secure integration obligation within contracts, ultimately forcing them to recertify all contracts and to some degree forcing new contracts or amendments should they ever move from [software platform] to another software.

This is the first time in all the times I've gone through audits that a required software call out was a point of nonconformance.

Response: Thank you for your inquiry.

Your answer appears to relate to the confidentiality requirement in Clause 4.1 and the secure transmission requirement in Accreditation Clause 4.5, most specifically the two highlighted sections below.

Clause 4.1 Public Record Researcher Agreement

> *CRA must have and follow a procedure requiring a signed agreement, which may include amendments and/or addenda, from all non-employee public record researchers. The agreement must clearly define the scope of services to be provided, including jurisdictions covered, search methodology, depth of search, disclosure of findings, methodology and time frame for communication and completion of requests, methodology for confirming identity of subject of record(s), confidentiality requirements, reinvestigation requirements, and other obligations as furnishers of information under the federal FCRA.*

Clause 4.5 Information Security

> *Organization / CRA must have and follow a procedure providing a secure means by which public record researchers will receive orders and return search results.*

While the Standard does not specifically require the Organization / CRA to name their third-party platform provider in their agreements with their public record researcher, it does require the agreements to contain provisions which specifically establish satisfaction of the confidentiality and data

security requirements. We appreciate that the Auditor is challenged to establish conformity in a situation where the Organization / CRA is not the ONLY entity that is responsible for the secure transmission of information. Ensuring the Agreement specifies and emphasizes "confidentiality of all consumer information", "secure data transmission", and "secure and timely disposal of confidential information."

Having said that, we believe that an Organization / CRA can establish conformity in different ways. Two possible methods of establishing conformity are outlined below:

1. The Organization / CRA's contract with the third-party platform provider should address topics like who is responsible for confidentiality of all private identifying information, masking, secure data transmission, data security standards, disposal of records, etc. In addition to the Organization -Platform contract, the Organization / CRA has a contract with a public record provider in which CRA describes the manner in which the Organization / CRA and the provider will transmit data between one another (via a secure third party platform specified by the Organization / CRA and subject to change from time to time) and requires with specificity that those transmissions will satisfy the terms of the Organization / CRA 's Agreement with their platform provider.
2. Same as (1) above only Organization / CRA chooses to specify the name of the third-party platform provider and specify and refer to that platform provider's obligations to deliver a means of confidential and secure transmission as well as to hold the public record researcher to the same standard.

In the case of example (1) above, the Organization / CRA would not need to specify the name of the third-party platform provider. In the case of example (2), the Organization / CRA could choose to specify the name of the third-party platform provider.

Please note, if your public record research agreements make no reference to these security and confidentiality requirements and the manner in which every party fulfills the obligations, then the Auditor will not be able to establish conformity. Opportunity for improvement could also be noted if a broad reference is made without specifying the obligations of each party to the arrangement.

Accordingly, naming the actual third-party platform provider in those Agreements is a reasonable attribute to look for in satisfaction of this requirement. However, this statement alone would not suffice without additional specifications contained in the Agreement describing what the Organization / CRA is doing (via that third party platform provider) to satisfy these confidentiality and data security transmission requirements. Furthermore, specifying the name of the platform provider is not necessarily required to satisfy these provisions.

The Accreditation Standard does not require the software provider be named in the contract between the Organization / CRA and the public record researcher.

Thank you for submitting your inquiry and giving the BSCC an opportunity to review. We believe we have responded fully to your inquiry. Please let us know if you have any further questions.

Issued November 2018
Reviewed July 2022
Reviewed August 2023