The Background Screening Credentialing Council

The Background Screening Credentialing Council volunteer members drafted the following response to several questions we have received about Information Security in Clause 1.1 of the BSAAP Standard, version 2.0, effective April 6, 2018 we have updated the responses to coincide with version 3.0 of the US Standard and version 1.0 of the Global Standard. This letter is an informal discussion of the question posed and does not constitute a legal opinion of the BSCC.

TITLE: Clause 1.1 – Information Security - PII

Question 1: I would like to pose a question regarding 1.1. I have spoken with ORGANIZATIONs and several platform providers who have asked the same question. They've heard the same answer and interpreted the same answer in different ways.

It is my reading that as long as 100% of electronically stored PII is held on servers that reside in a facility that is certified against one of the acceptable standards, then the requirement is met. This can be a data center facility operated by the CRA, a data center operated by a platform provider, or a data center operated by a third party.

The audited entity is the entity where the PII is held.

The certificate of the audit of the entity holding the PII must be presented by the CRA to fulfill 1.1. Is my reading of Clause 1.1 correct?

Response: Thank you for your inquiry regarding Clause 1.1 of the PBSA Accreditation Standard and Audit Criteria, version 3.0, (effective date TBD).

Based on feedback and the recent open comment period related to our upcoming General – Global Standard V.1.0, it became evident that this clause required further clarification. Under both Accreditation Standards, Clause 1.1 now focuses on the "system" component of this requirement, versus the "location" where the information is held. The system should be thought of as the software that contains the PII. This should more directly move the discussion away from servers.

Please be aware that Clause 1.1 now reads as follows:

1.1 Information Security Certification

Any system (i.e. platform, application, database) which is used to store and access Personally Identifiable Information (Personal Data) whether with the organization, and/or organization's platform provider (whether internal or hosted) must hold a current (current as defined by the certifying body) information security certification and/or provide written evidence of completing an information security audit for which no critical, high-risk, or severe security vulnerabilities remain uncured. The source of such certification and/or written evidence must be a qualified security assessor.

The drafting of this clause considers the various scenarios that exist for organizations who would be seeking accreditation. Those scenarios may include, for example, organizations who use a third-party

screening platform, organizations who own and operate their own proprietary platform, organizations who own and operate several proprietary platforms, and/or a combination of a third-party and proprietary platforms.

For the sake of responding, we have crafted two common examples of how Clause 1.1 might be applied:

SCENARIO 1: An organization contracts with an industry-wide platform provider to deliver background screening services to organization's clients. Platform provider owns, controls and operates its own proprietary software on servers that platform provider owns and operates. Platform provider's servers are stored pursuant to a June 2018 data center lease in a Tier 2 data center. The organization holds no PII on its own locally operated servers.

Under this scenario, the organization seeking accreditation would not be required to produce an information security certification specific to their organization. Rather, the organization would produce proof of an information security certification of the servers and software platform owned and operated by the third-party platform provider. Depending on the third-party platform provider structure, a single information security certification may encompass all three items (servers, third-party platform, and data center hosting servers). The organization will also need to provide proof of the contractual relationships between the parties involved (organization, Platform Provider, and Data Center if separate from Platform Provider).

NOTE – the tier level of data center is not defined in this Clause of the Standard and does not impact the response from the BSCC. The key determination is whether the servers are housed within the organization or at an external, colocation data center facility.

NOTE: If the organization holds PII outside of this third-party platform, for whatever system houses the PII, the organization must provide evidence of information security certification for: 1) the hardware and software platform holding the data, 2) the physical facility where the data is stored, and 3) if third-parties hold and/or provide physical facility for holding the data, the contractual relationship between the parties.

SCENARIO 2: Organization owns and operates its own proprietary software and stores it on servers that it owns and operates and are located in a Tier 2 data center facility pursuant to a data center lease with organization.

Under this scenario, organization would provide proof of information security certification of the platform and servers that it owns and operates

In summary, to meet the requirements of Clause 1.1, the organization must provide evidence of information security certification for: 1) the hardware and software platform holding the data, 2) the physical facility where the data is stored, and 3) if third-parties hold and/or provide physical facility for holding the data, the contractual relationship between the parties.

Question 2: "Wherever PII is held" means in this clause "Wherever PII is digitally held", correct?

Response: Yes; "digitally held" is correct.

Question 3: "The audit needs to apply not only to the entity holding the PII, but also the entity that operates/owns the servers, correct?

Response: We interpret your question as meaning “The certification needs to apply…” In that case, the entity/s holding, owning, and/or operating the servers must hold an information security certification per the specifications provided in Clause 1.1. A more detailed response, including examples, is found in the answer to Question 1 above.