The Background Screening Credentialing Council

The Background Screening Credentialing Council volunteer members drafted the following response to a question about Information Security in 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: Clause 1.1 – Information Security - PII (Part 1 of 2, published June 2018)

Question: I would like to pose a question regarding 1.1. I have spoken with CRAs 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 NAPBS Accreditation Standard and Audit Criteria, version 2.0, that went into effect as of April 6, 2018. Let us start by clarifying that Clause 1.1 now reads as follows:

1.1 Information Security Certification
Wherever Personally Identifiable Information (PII) is held, whether at CRA, CRA's data center (whether internal or hosted), and/or CRA's platform provider (whether internal or hosted) such entity 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.

As we drafted this standard, the BSCC carefully considered the various scenarios that exist for our varying members who would be seeking accreditation. Those scenarios may include, for example, small CRAs who use a third-party screening platform, medium-sized CRAs who own and operate their own proprietary platform and larger CRAs who may own and operate several proprietary platforms.

For the sake of responding, we have crafted two commonplace examples of how Clause 1.1 might work:

SCENARIO 1: CRA contracts with an industry-wide platform provider to deliver background screening services to CRA'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

data center lease in a Tier 2 data center. CRA holds no PII on its own locally operated servers. All PII is contained within the third party platform.

Under this scenario, CRA would not be required to produce an information security certification specific to CRA organization. Rather, CRA would produce a proof of information security certification of the servers and software platform owned and operated by the third-party platform provider. Additionally, Platform provider must provide proof of information security certification of the data center facility, whether owned by the platform provider or a third-party, to CRA. CRA would submit proof of servers, software platform, and data center where data is held having the proper certifications. 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 CRA will also need to provide proof of the contractual relationships between the parties involved (CRA, Platform Provider, and Data Center if separate from Platform Provider).

SCENARIO 2: CRA owns and operates its own proprietary software and stores it on servers that it owns and operates but which are located in a Tier 2 data center facility pursuant to a data center lease with CRA. Under this scenario, CRA would provide proof of information security certification of the platform and servers that it owns and operates. The Data center facility would provide proof of its information security certification to CRA. CRA would submit both the data center facility certification and its own certification together with the data center lease as evidence of its conformity with Clause 1.1.

In summary, to meet the requirements of Clause 1.1, CRA 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.

We hope this additional insight assists you in your preparation for the accreditation audit process, and that by making this available through our published opinion letter process, we are able to provide clarity to other organizations as well.

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

The Background Screening Credentialing Council

The Background Screening Credentialing Council volunteer members drafted the following response to questions about Information Security in 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: Clause 1.1 – Information Security - PII (Part 2 of 2, published October 2018)

Thank you for your inquiry regarding Clause 1.1 of the NAPBS Accreditation Standard and Audit Criteria, version 2.0, that went into effect as of April 6, 2018. As your three questions all relate to Clause 1.1, we are addressing them in [this] single opinion letter.

Clause 1.1, v2.0 reads as follows:

1.1 Information Security Certification
Wherever Personally Identifiable Information (PII) is held, whether at CRA, CRA's data center (whether internal or hosted), and/or CRA's platform provider (whether internal or hosted) such entity 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.

Question 1: "*Wherever PII is held" means in this clause "Wherever PII is digitally held", correct?*

> **Response to Question 1:** Yes; "digitally held" is correct. For a more detailed response, including examples, please see an earlier Opinion Letter, Clause 1.1 Information Security - BSAAP Standard, v 2.0, Effective April 6, 2018.

Question 2: "*The audit needs to apply not only to the entity holding the PII, but also the entity that operates/owns the servers, correct?*

> **Response to Question 2:** 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. As noted in our response to Question 1, a more detailed response, including examples, is found in an earlier Opinion Letter, Clause 1.1 Information Security - BSAAP Standard, v 2.0, Effective April 6, 2018.

Question 3: *"The term "qualified security assessor" does not necessarily mean a PCI Security Council certified firm, correct? Rather this can mean a truly independent entity whose business is to perform these types of audits. CRA is responsible for performing due diligence, obtaining references, etc. Correct?*

> **Response to Question 3:** Yes; a "qualified security assessor" does not require a PCI Security Council certified firm. Please note the column entitled "Attributes of and Suggestions for Onsite Audit" for Clause 1.1, which provides two alternatives for demonstrating compliance, noting the bolded text.

Wherever Personally Identifiable Information (PII) is held, whether at CRA, CRA's data center (whether internal or hosted), and/or CRA's platform provider (whether internal or hosted) such entity must hold a current (current as defined by the certifying body) information security certification or written evidence of information security audit by a qualified security assessor for which no critical, high-risk, or severe security vulnerabilities remain uncured. Examples of acceptable certifications/audits include, but are not limited to: 1) ISO 27001:2013, 2) SOC 2 (Type II), 3) EI3PA, 4) NIST SP 800-37 and NIST SP 800-53 rev 4, and PCI. ***Alternatively, written evidence of audits will be acceptable if: 1) certification document is provided, 2) audit results signed by auditor show no critical, high-risk, or severe security vulnerabilities remain uncured, or 3) signed attestation from auditor including date of audit, name of qualified security assessor, name of auditing company, statement that no critical, high-risk, or critical security vulnerabilities remain uncured, and 4) name of security standard/s used as basis for auditing.***

It is expected the CRA will conduct due diligence on the information security auditing firm and will provide evidence of such due diligence.

We hope this additional insight assists you in your preparation for the accreditation audit process, and that by making this available through our published opinion letter process, we are able to provide clarity to other organizations as well.

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