BSAAP Standard Proposed Revisions
Comments submitted during Public Comment Period
July 27, 2020 – August 26, 2020

Below is a list of comments received in response to the proposed BSAAP Global Standard and revisions to the existing BSAAP v2 Clauses 1.1 and 1.4.

	Global-General Standard
Clause	**Comment**
General	Could you please advise whether it is recommended to seek the accreditation: (i) of the head office pursuing client relationships and management of the foreign entities of the Group under the Global Accreditation Standard; (ii) of the all the Group companies pursuing client relationships under the Global Accreditation Standard or US Accreditation Standard, or (iii) of the US subsidiary under the US Accreditation Standard.
General	If a CRA primarily outsources its international screening, are they eligible for international accreditation?
General	What is the timeline for releasing this outside the USA?
General	What are the expected fees and other operational aspects such as the identity of the accreditation body etc.
1.1	*See US Standard 1.1 Comments on US Standard*
1.2	I think this number is missing for the "Designate one or more individuals…" on the spreadsheet.
2.8	Will we be required to either obtain a new client agreement or addendum from every client regarding data protection regulations?
2.9	Client Legal Responsibilities Per the [Could you please confirm wording], current legal responsibilities include: 1) having permissible purpose, 2) disclosing to subject, 3) obtaining subject authorization, 4) following prescribed adverse action procedures, 5) complying with all applicable legal and regulatory requirements, and 6) obtaining, retaining, using, and destroying data in a confidential manner.
2.9a	Use Limitation: This policy seems to imply that an organization would never be a controller. Some organizations may view themselves as controllers and may enter into a controller-to-controller data sharing agreements, versus processor-to-controller. I would recommend inserting the word "processor" after each appearance of the word "controller" in this policy section.
2.14	This policy appears to be an adaptation from the U.S. standard, which in turn implements § 1681k of FCRA; however, the Global standard considerably expands beyond the U.S. standard. For example, the U.S. standard is limited to public record information which is

	likely to have an adverse effect on a consumer's ability to obtain employment, but there is no such restriction in the Global standard. It is not limited to public records, and it is not limited to scenarios involving employment. What would be the reason for this expansion? The Global standard also appears to inject § 1681e accuracy requirement that is not present in the U.S. standard or § 1681k. I recommend removing the requirement that the record must be reported "accurately from the source" and narrowing this to the employment context only. Accuracy is already addressed in Standard 2.19.
2.14	Was the option to notify the consumer purposely omitted, unlike the domestic standard? I have no problem if that was intentional—just want to ensure it was intended
2.15	Although this is admittedly a redundancy that is also contained in the U.S. standard, I'm not sure why an organization should be required "to have procedures . . . requiring reasonable procedures." It would seem to be the case that an organization should simply "have and follow reasonable procedures to assure maximum possible accuracy." The clause requiring the organization to "use all reasonably available information to ensure the data being reported can be matched to the subject" when there is a name search only service imposes a vague and subjective standard. What constitutes "all reasonably available information?" What does it mean to "use" that information? What law, regulation, or custom requires this standard? If an organization is making an identity match based upon a full name and date of birth, may it disregard other (possibly contrary) information that is still reasonably available? Why are global organizations being held to a standard that is different than U.S. organizations in this particular area?
2.16	The second column seems to assume that an organization is only a processor; organizations may view themselves as controllers. This policy also seems to assume that an organization is obligated to provide all information in the subject's file. What is the definition of the term "file" in this context? I assume it does not have the same definition as what is given to a consumer file here in the U.S.? In the U.S., there is definitional ambiguity over the term "file," and there are items of information that relate to the consumer which are not considered to be part of the file. By use of the concept of file in a non-consumer reporting agency context, doesn't this standard create ambiguities and impose obligations that would not otherwise be imposed upon organizations? I would recommend restructuring the standard to state something along the following lines: If required by applicable laws and regulations, organization must have and follow procedures for documenting and responding to a subject's request for information on that subject that is possessed or maintained by the organization or, if appropriate, referring the data subject to the client, end-user, controller, or joint controller.
2.20	Re-appearance of Inaccurate Information: The word "permitted" in this clause should be removed and the word "required" should be substituted. Also, the word "customer" is used in this standard, but the word "client" is used elsewhere. For clarity, I recommend consistent use of one term only.
3.3	Understanding Subject Reports. 3) the subject report retention and destruction practices as outlined in the Fair Information Privacy Principles. [Could you please confirm the reference] (...) Methods include, but are not limited to, inclusion in Client agreement, User agreement or through some other document which is signed by the client and includes, but is not limited to, client acknowledgement of subject data protection responsibilities. Per the FIPPs [Could you please confirm the reference], current requirements include: 1)

	limiting dissemination of subject information to only those with legitimate need, permissible purpose, and authorized by subject; 2) retaining subject data in a confidential manner; and 3) destroying data in a secure manner.
3.4	Information Protection: I would recommend inserting the prepositional phrase “if any" after the word “requirement.” The phrase “Fair Information Privacy Principles” is not defined. Does this refer to the Fair Information Practice Principles? Does the BSCC mean to incorporate an entire external standard? If so, I would recommend a clear reference to the governing body that promulgates and updates those standards. What if this external standard evolves in such a way that it adopts principles and practices with which we disagree?
4.6	While the phrase “where allowable by law or source” is listed, does re-using subject data in general put companies at odds with the GDPR and other data privacy laws? When auditing records, we test them against other vendors/sources, so there are many searches that require special applicant permission or forms, which would limit what searches could even be audited. There is also the cost factor, as international searches are usually significantly higher
5.1	Verification Accuracy: I'm not clear on what is to be understood by the use of the term “search information” in lieu of the term “verification information.” The title of this standard is “Verification Accuracy” and the standard pertains to verification services. What is served by removing the word “verification” from the text of the standard? Does this have a different scope or application than the U.S. standard?
Various Grammar	2.1 I believe there is a number missing for the “The organization must conduct and assessment in their role(s)…” 2.2 The numbering jumps from 2.2 to 2.6 with one clause between that is numbered. 2.6 There are two 2.6 clauses and a missing 2.7. 2.12 Is missing. 4.3 I think the number is missing and there is no 4.4 5.5 And 5.6. The reason you don’t just combine these is that 5.5 refers to verifications and 5.6 refers to jurisdictions and you cannot combine into one clause? 6.12 This will be duplicative of 1.3, attribute 7, right?

	US Standard Clauses 1.1 and 1.4
Clause	**Comment**
1.1	The proposed changes do not seem to be substantially different, but rather seem to emphasize that the information security certification can be done by a qualified 3rd party that is not necessarily using one of the named security standards, the names of which are being omitted. Correct?
1.1	This is still the clause that generates the most questions and I think the reason is that the wording of the clause may not state what the clause means—or it may mean exactly what it says, but two subsequent opinion letters seem to be in conflict The clause language states: Wherever Personally Identifiable Information (PII Personal Data) is held, whether at organization, organization's data center (whether internal or hosted), and/or organization'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. [Emphasis added.] So while the clause states "wherever…held" one opinion letter makes clear that it is more than that. It is wherever PII is held and/or controlled.
1.1	"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. [Emphasis added] https://pubs.thepbsa.org/pub.cfm?id=5DB7E655-B751-2877-0F75-668E22BD6EC5 However, another opinion letter discusses whether the CRA must have a security certification or only the data center that holds the information. Thus, holding your PII data (from a digital standpoint) at a data center that holds a current an active SOC II (Type II) certification, does satisfy Clause 1.1 of Accreditation Standard 2.0. We do think it is important to note that in addition to satisfying Clause 1.1. re: Information Security Certification, accredited agencies must also satisfy the rest of the clauses surrounding Information Security and set forth in Clauses 1.2 through 1.12. Together, these clauses set forth requirements for a comprehensive Information Security policy that includes appropriate data access, storage, backup, security, masking, destruction and related information security practices. https://pubs.thepbsa.org/pub.cfm?id=D8CAD7B4-E9AB-2E3E-0E38-32620C2E3A86

	So here is appears that it is indeed just the entity that holds the data, not both entities, i.e., the one entity “holds” the data while the other “owns/and or operates” the servers. (Needless to say, the CRA must comply with all other security clauses either way.) So, I think the BSCC has an opportunity to clear this up—either by modifying the clause wording or purposefully leaving as is. If you leave the clause wording as is, the second opinion letter above is correct. “Thus, holding your PII data (from a digital standpoint) at a data center that holds a current an active SOC II (Type II) certification, does satisfy Clause 1.1 of Accreditation Standard 2.0.” The clause says what it means: “Where the PII is held.” On the other hand, if the first opinion letter above is correct: ” 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.” The clause wording should be changed to: Wherever Personally Identifiable Information (PII Personal Data) is held and/or operated or controlled, whether at organization, organization’s data center (whether internal or hosted), and/or organization’s platform provider (whether internal or hosted) such entity(s)… So, by leaving the language as is, it could be read to mean what it says. If that is not strictly what is meant it could be made clear in the clause language with the above modification and put a lot of questions to rest. The proposed changes do not seem to be substantially different, but rather seem to emphasize that the information security certification can be done by a qualified 3rd party that is not necessarily using one of the named security standards. The clause language states: Wherever Personally Identifiable Information (PII Personal Data) is held, whether at organization, organization’s data center (whether internal or hosted), and/or organization’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: What defines a qualified security assessor? Does this include Vulnerability Management Platforms/Software? **1.1.Suggestion for Improvement** Allow a third option to be included that meets the desired result of the standard but is affordable to all. This can be done through Vulnerability Management Platform/Software. Overview of Vulnerability Management Platforms/Software

	Allowing CRAs to use such a Vulnerability Management Platform/Software solution as a means ofmeeting the standard will actually strengthen the Pre-employment Background Screening industry. Most CRA's will never see these security gaps until it is either too late and they have a breach, or until their next audit. If found at the audit level, the costs really begin to build for the CRA through network support engineers, PEN test remediation, and then retesting. By allowing the CRA to leverage a Self- Audit Management platform they will automatically discover vulnerabilities in a more timely manner there by preventing the breach and thus helping the overall credibility of the market. Benefits of the Vulnerability Management Platforms/Software include: Alerts to file changes, deletions, or failed attempts at access of critical data. Threat patters are constantly updated and analyzed against your network activity. These solutions can be scaled to the needs and size of the business. These data security tools are actually a better fit for most CRAs because they provide support and often explain the vulnerability in terms that actually allow the CRA to fix the issue. Many of the Vulnerability Management Platforms have built in reporting for proof of audit activities and standards that include SOC2, NIST, ISO27002, HIPPA and more. In other words, the reports that are generated from the penetration testing are equal to what a third-party auditor would produce but at a significant cost savings. CRA can automate data discovery and classification, as well as review who has access and how it is used. Vulnerability Management Platforms/Software range from $2,000 a year and up depending on wants and needs. Accreditation should be attainable for those who work hard to achieve the honor and should not be unreasonably costly. It should be equally attainable to all CRA's regardless of size. It may have been the BSCC's intention to include Vulnerability Management Platforms/Software under this standard, but more clarification is needed. If it was not BSCC's intention to include this type of remedy, then perhaps Vulnerability Management Platforms/Software should be considered as a viable third option. The word "held" can be understood as "physically located" or "controlled." It is typical for a server holding data to be physically located in a co-location facility (data center) owned by one party but controlled by a second party. In such a case, the co-location facility has primary responsibility for physical security, while the CRA or platform provider has primary responsibility for logical security. Does this clause require both entities to be certified by a qualified security assessor? I am assuming that the answer is, yes, as both roles are essential in keeping data secure. . . . 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. There is no definition for what constitutes a qualified security assessor. Is this judgment left to the discretion of the auditor?
1.4	Clause Language Addition:

	In the event of a breach, a CRA should have documented recovery/business resumption procedures. This seems more of an “attribute” that the auditor would review for the added “recover” in the clause itself. However, if you do leave as is, I would add this requirement to your attributes that the auditor will audit. The recovery plan would seem to have to be very general as prior to the occurrence, it is not known what details are that the CRA is recovering from—which could affect the plan. Attribute for onsite audit addition: (7 an implementation plan for any required remediation, An implementation plan for required remediation seems to be premature before knowing what needs to be remediated. I would suggest something of like “requiring the creation of an implementation plan once any required remediation determined.”