The Background Screening Credentialing Council

The Background Screening Credentialing Council volunteer members drafted the following response to questions about 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 1.12 – Truncation of SSN and Other Sensitive Data Elements

Question

In looking at the clause for 1.12, it states the CRA must have and follow a procedure to suppress or truncate Social Security Numbers and other sensitive data elements ***as required by law****. Do you know what law this is in reference to? We've looked at the FCRA and DPPA text and do not see this requirement anywhere. We have also checked the Social Security regulations and cannot find it there either. The only thing we've found is a bill that referred to the subcommittee on Social Security in 2016.* *https://www.congress.gov/bill/114th-congress/house-bill/4546/text*

Response

Thank you for submitting your inquiry and giving the BSCC an opportunity to respond to it.

You have inquired about the basis for the requirement in Clause 1.12 relating to truncation of Social Security Numbers and other sensitive data elements

The standard articulated in Clause 1.2 regarding truncation of Social Security Numbers (i.e. to only show the last 4 identifying digits of the number) originally arose out of "The Principle of Least Privilege" which is an important concept in information security, is the practice of limiting information access rights for users to the bare minimum permissions they need to perform their work. Under the principle, system users are granted permission to read, write or execute only the files or resources they need to do their jobs: In other words, the least amount of privilege necessary. In the case of an individual's Social Security Number, granting access to more than the last 4 digits of the number are not necessary and pose a risk of identity theft if access were granted widely. The principle and industry practice established has been supported by courts and has become an established common law (not written into a statute necessarily but recognized and upheld by a variety of state and federal courts).

In addition, many state Courts codified the principle into state statutes. The National Council of State Legislatures published a list of the state laws in effect as of 2010 (about the time of some of the early drafting of the BSAAP Standards) which as of the writing of this opinion letter can be found on their public-facing website here.

In 2014, the IRS issued final regs (**T.D. 9675**, "2014 regs") authorizing the use of truncated taxpayer identification numbers (TTINs) on certain payee statements and certain other documents (W-2s including regarding payment of wages in the form of group term life insurance) or where specifically allowed. The 2014 regs were in response to concerns about the risks of identity theft, including its effect on tax administration. **Reg. § 301.6109-4(b)** generally provides that a TTIN may be used to identify any person on any statement or other document that the internal revenue laws require to be furnished to another person. Under **Reg. § 301.6109-4(a)**, a TTIN is an individual's SSN, IRS individual taxpayer identification number (ITIN), IRS adoption taxpayer identification number (ATIN), or IRS employer identification number (EIN) in which the first five digits of the nine-digit number are replaced with Xs or asterisks. For example, a TTIN replacing an SSN appears in the form XXX-XX-1234 or ***-**-1234.

More recently, in July of 2017, the United States Government Accountability Office (GAO) issued a report to the Chairman Subcommittee on Social Security Committee on Ways and Means House of Representatives which specifically directs that all government agencies should take measures to reduce the collection, use and display of private identifying information, including truncating social security numbers so as to limit identity theft risks. See https://www.govinfo.gov/content/pkg/CFR-2015-title26-vol20/pdf/CFR-2015-title26-vol20-sec301-6109-4.pdf (hereafter "2017 GAO Report").

The 2017 GAO Report discusses key laws that provided the legal framework for the Government to protect SSNs and other PII; including the Privacy Act of 1974 (requiring that agencies maintain only those records containing PII that are "relevant and necessary" to accomplish agency purposes) and the implementing regulations, and the E-Government Act of 2002 (requiring agencies to conduct privacy impact assessments before developing or procuring information technology that collects, maintains or disseminates information that is in identifiable form, such as SSNs) and its implementing regulations. Additionally, the OMB has issued numerous guidance on other information security and privacy-related issues including federal agency website privacy policies, interagency sharing of personal information, designation of senior staff responsible for privacy, data breach response and notification, and safeguarding PII.

While these federal laws, regulations and guidelines only directly govern the agencies of the federal government, they offer a framework for how to protect privacy in the context of developing and implementing information technology as well as operational systems/policies/procedures/practices. This body of law recognizes and establishes a practice of truncation of social security numbers (as well as other private identifying information) that has strengthened and spread to private industry as the use of technology has proliferated.

In response, therefore, to your inquiry, the BSCC has adopted in Clause 1.12 the longstanding data privacy and protection practice of truncation of sensitive data elements *AND* has left open the possibility that as the privacy laws develop, more state and/or federal requirements may arise over time. As with other matters, it is the responsibility of the accredited firm to monitor these changes in the laws and to adjust their privacy practices accordingly. Conformity with Clause 1.12 does require it.

We believe we have responded fully to your inquiry and have offered some insight into the legal basis for the requirements in Clause 1.12. Please let us know if you have any further questions.