The Background Screening Credentialing Council (BSCC) volunteer members drafted the accreditation tip for Clause 1.2 of the BSAAP Standard, version 2.0, effective April 6, 2018. This tip does not constitute a legal opinion of the BSCC.

TITLE: Clause 1.2 – Information Security Policy

Clause: CRA must have and follow a written information security policy which, at a minimum, complies with applicable law and regulation. CRA must designate one or more individuals responsible for implementing, managing and enforcing the information security policy (individual(s) may be internal or contracted).

A **Non-Conformity** for section 1.2 may look something like the following:

> *"Testing of the control activity disclosed that the entity did not have an executed service level agreement in place with the third-party managed services provider they are contracted with. The vendor provides managed services that includes, but is not limited to, setting up new users, workstations, and regular maintenance on the entity's firewall. The entity categorized the managed services vendor as an "as needed" service provider."*

The Audit Criteria for Clause 1.2 of the BSAAP Standard, Version 2.0, Effective April 6, 2018 provides:

This is an overarching information security policy which broadly addresses security within the CRA environment. This policy may reference other security policies and/or procedures dealing with specific security topics. Such document(s) must, at a minimum, address: 1) key personnel, roles and responsibilities, 2) policy changes and modifications, 3) system configuration, 4) anti-virus, firewall, and router configuration, 5) data and information classification, 6) encryption, 7) access control, 8) electronic data retention, storage, and disposal, 9) paper and hard data retention, storage, and disposal, 10) data device retention, storage, and disposal, 11) incident response, 12) physical security, and 13) security policy revision history. Auditor will seek evidence of adherence to policy.