BSAAP Standard with Audit Criteria, version 2.0 (Updates to Clauses 1.2 and 4.5)				
Section	**Clause**	**Measure & Documentation Typically subject to Desk Audit**	**Potential Verification for Onsite Audit**	**Attributes of and Suggestions for Onsite Audit (What auditor will look for in policy, procedure, activity)**
1 Information Security	**1.2 Information Security Policy** 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).	CRA must provide written information security policy.	CRA must present written information security policy and provide evidence of adherence to such policy. If questioned, CRA workers must demonstrate knowledge of information security policy and be able to access current policy.	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, and 14) Remote Workforce Policy. Auditor will seek evidence of adherence to policy.

1 Information Security	**1.2 Information Security Policy** Designated individual must have the required authority and independence to fulfill their duties under this Clause. Designated individual must be insulated from adverse employment actions resulting from the competent execution of their duties	CRA must employ or retain a minimum of one person who is responsible for CRA's overall information security program. This must be evidenced by written job description, policy, procedure, executed agreement or other documentation. If various people are responsible for different aspects of the program, one person must hold overall responsibility as evidenced by job description, organizational chart, or other documentation.	CRA must present written job description, policy, procedure or other documentation which identifies, by name and title, the person responsible for the overall information security program. If questioned, CRA workers must identify individual responsible for overall information security program.	CRA must present documentation which clearly identifies person, by name and title, responsible for overall information security program.

4 Researcher and Data Standards	**4.5 Information Security** CRA must have and follow a procedure providing a secure means by which public record researchers will receive orders and return search results.	CRA must provide written policy, procedure, or other written documentation describing the requirement to and method used to secure and protect consumer information when such information is being transmitted to and returned by public record researchers.	CRA must present written procedure for sending consumer information to and receiving consumer information from public record researchers and obtain signed agreement from researcher to that effect. CRA must make available the person responsible for security of transmitted consumer information. For each transmission method, CRA may be asked to demonstrate, or provide written documentation of, the security controls which are in use. CRA must provide evidence of adherence to procedures.	Security procedures, which must be agreed to in writing by researcher, for transmission of personally identifiable information to/from public record researchers must include, but are not limited to use of an electronic system designed for secure transmission of information between CRA and researcher; or if other transmission methods are used, security procedures must include, but are not limited to: 1) all transmissions must be directed to a named party, 2) all transmissions must be clearly marked as "CONFIDENTIAL" and include a request to notify sender if received by someone other than named party, 3) if faxed, a cover page must always be used and must not contain any personally identifiable information, 4) if faxed, CRA must have verified receiving fax is in a non-public location, 5) ~~if transmitted using CRA network, such network must be secured using a minimum of 128 SSL, 6)~~ if transmitted via Internet, data must be securely encrypted ~~or protected in a comparable manner~~ using a currently recognized standard. Auditor will seek evidence of adherence to policies and procedures.