NAPBS BACKGROUND SCREENING AGENCY ACCREDITATION PROGRAM – ACCREDITATION STANDARD AND AUDIT CRITERIA (Glossary provided at end of document.)

Version 2.0

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)
Information Security			
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.	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 completion of information security audit for which no critical, high-risk, or severe security vulnerabilities remain uncured. Written evidence must include name of security standard used as basis for auditing and at least one of the following from a qualified security assessor: 1) certification document, 2) audit results signed by auditor showing no remaining uncured critical, high-risk, or severe security vulnerabilities, or 3) signed attestation including date of audit, name of auditor/s, name of auditing company, and statement that no critical, high-risk, or severe security vulnerabilities were found or, if found, such vulnerabilities have been cured.	CRA, CRA's data center (whether internal or hosted), and/or CRA's platform provider (whether internal or hosted) must provide evidence from a qualified security assessor of current information security certification or completion of information security audit for which no critical, high-risk, or severe security vulnerabilities remain uncured.	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.
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. Auditor will seek evidence of adherence to policy.
	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	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.

NAPBS BACKGROUND SCREENING AGENCY ACCREDITATION PROGRAM (BSAAP) – ACCREDITATION STANDARD AND AUDIT CRITERIA

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)
	job description, organizational chart, or other documentation.		
1.3 Data Security			
CRA must have and follow procedures to protect consumer information under the control of the CRA from internal and external unauthorized access. These procedures must include specifications for the securing of information when electronically transmitted, as well as information in both hard copy and electronic form including information stored on portable and/or removable electronic devices. At a minimum, procedures must meet all applicable legal and regulatory requirements.	CRA must provide written procedures to protect consumer information from unauthorized electronic and/or physical access. This includes the collection, use, storage, transmission, and destruction of consumer information in both paper and electronic form.	CRA workers dealing with consumer information must be able to explain and demonstrate procedures for protecting consumer information in their possession, whether such information is used internally and/or externally, be able to access current documentation, and provide evidence of adherence to such procedures. CRA must also be able to demonstrate electronic and physical protection of consumer information. CRA must provide evidence of adherence to such procedures.	The policies and procedures designed to protect consumer information must include, but are not limited to, the following: 1) securing unattended workstations, 2) limiting access to networks, data, and work areas, 3) limiting consumer information provided to information sources to only that information which is needed for a specific business purpose, 4) destruction of hard copy documents, 5) identification of caller before providing consumer information, 6) employee badging or other identification system, 7) unescorted visitor policy, 8) secure document destruction, 9) secure transport of information, 10) use of encryption and/or secure networks and/or websites, 11) control of access to consumer information, 12) controlling use of portable storage devices, 13) alarm systems, 14) door locks, and 15) secure server and back-up sites. Auditor will seek evidence of adherence to policies and procedures.
1.4 Intrusion and Data Security			
CRA must have and follow procedures to prevent, detect, investigate and respond to an information system intrusion, including consumer notification and other breach notifications where mandated. At a minimum, procedures must meet all applicable legal and regulatory requirements.	CRA must provide procedures for preventing, detecting, identifying and responding to information system intrusions (unauthorized access to computer systems and/or consumer data).	CRA must make available the procedure, process, and tools used to prevent unauthorized access, monitor access and identify potential intrusions; CRA must provide evidence of adherence to such procedures.	CRA must present proof of tools used to protect network, data, and consumer information. This may be third-party audit results, intrusion/detection testing results, firewall protections used, website security, or other recognized security protocols and devices. Auditor will seek evidence of adherence to policies and procedures.
	CRA must provide procedures for responding to information system intrusions including how consumer notification and other breach requirements are determined.	CRA must make available the procedure, process, and/or tools used to respond to intrusions. If questioned, CRA workers must demonstrate knowledge of procedure to be followed in case of intrusion or suspected intrusion and be able to access current documentation. CRA must provide evidence of adherence to such procedures.	Process/procedure must include, but is not limited to: 1) individual to contact in case of intrusion and his/her back-ups, 2) necessity of immediately stopping intrusion activity, if still occurring, 3) determination of notification requirements, 4) preparing notification/s, 5) obtaining necessary approvals of notification language, 6) communicating notification, and 7) de-brief to prevent future occurrences. Auditor will seek evidence of adherence to policies and procedures.
1.5 Storage and Backup of Data			
CRA must have and follow procedures to ensure data is backed up and stored in an encrypted or otherwise protected manner. At a minimum, procedures must meet all applicable legal and regulatory requirements.	CRA must provide written policy, procedure or other documentation explaining data backup, storage, and access procedures.	CRA must make available the procedure, process, and/or tools used to manage data backup and storage. CRA must make available the individual responsible for data backup and storage. This individual must be able to describe and provide documentation related to backup and data storage. CRA must provide evidence of adherence to	The process used to backup and store data must include, but is not limited to: limiting access to backup data to select authorized individuals, secure transport of backup data to storage location (including virtual storage), and security at the storage location. At a minimum this includes locked storage facility (if physical building is used), secure access protocols, and compliance with all applicable legal and regulatory requirements. Auditor will seek evidence of adherence to policies and procedures.

NAPBS BACKGROUND SCREENING AGENCY ACCREDITATION PROGRAM (BSAAP) – ACCREDITATION STANDARD AND AUDIT CRITERIA

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)
		procedures.	
1.6 Access Protocol			
CRA must have and follow procedures requiring use of secure access protocols for CRA workers, authorized client users, and any other authorized users accessing Consumer Information. At a minimum, procedures must meet all applicable legal and regulatory requirements.	CRA must provide written policy, procedure, or other documentation which explains access protocols for CRA workers and authorized client users with access to consumer information.	CRA must make available the individual responsible for access protocol. This individual must be able to describe and provide documentation related to access protocols including assignment, replacement, and recordkeeping. If questioned, CRA workers with access to consumer information must explain process to obtain access for him/her and/or authorized client users and be able to access current documentation. CRA must provide evidence of adherence to procedures.	CRA must demonstrate that access to consumer information by CRA workers and authorized clients users is controlled. Acceptable access protocols may include, but are not limited to, strong passwords, biometric identification, and/or multi-factor identification. Records of access protocol issuance must be securely maintained. Auditor will seek evidence of adherence to policies and procedures.
1.7 Electronic Access Control			
CRA must have and follow procedures to control access to all electronic information systems and electronic media that contain consumer information. CRA must have procedures in place to administer access rights. CRA workers and authorized client users must only be given the access necessary to perform their required functions. Access rights must be updated based on personnel or system changes.	CRA must provide written policy, procedure or other documentation explaining how access rights to consumer information by CRA workers and authorized client users are controlled and administered.	CRA must make available the individual responsible for controlling access to consumer information. This individual must be able to describe and/or provide documentation and/or provide a demonstration related to access control. If questioned, CRA workers who receive requests for access to consumer information will demonstrate knowledge of process to add or change access rights for CRA workers and authorized client users. CRA must provide evidence of adherence to procedures.	Process must include, but is not limited to: 1) how CRA workers and authorized client users apply for and receive access, 2) authorization needed for access, 3) access parameters, 4) issuance, replacement, and expiration of access rights, 5) monitoring tools, and 6) recordkeeping. Auditor will seek evidence of adherence to policies and procedures.
1.8 Physical Security			
CRA must have and follow procedures to control physical access to all areas of CRA facilities, including data storage facilities that contain consumer information.	CRA must provide written policy, procedure or other documentation explaining how access to areas of CRA facilities containing consumer information is controlled for CRA workers, vendors, and guests and how records of such access are maintained.	CRA must provide auditor a tour of the facility, demonstrating and describing the physical security measures in place. Auditor may interview CRA workers about physical security procedures and, if questioned, workers must describe physical security protocols and be able to access current documentation. CRA must provide evidence of adherence to procedures.	Process/procedure must cover CRA workers, vendors, and guests, and include, but not be limited to, the following: 1) procedures for granting levels of access to CRA workers (e.g., assignment of keys or security system passcodes), 2) procedures for authorizing and monitoring guests (including the auditor) to the facility, and 3) control of access by CRA workers, vendors, and guests. Auditor will seek evidence of adherence to policies and procedures.
1.9 Consumer Information Privacy Policy			

NAPBS BACKGROUND SCREENING AGENCY ACCREDITATION PROGRAM (BSAAP) – ACCREDITATION STANDARD AND AUDIT CRITERIA

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)
CRA must have and follow a Consumer Information Privacy Policy detailing the purpose of the collection of consumer information, the intended use, and how the information will be shared, stored and destroyed. The CRA must post this policy on its website, if it has one. CRA must have and follow procedure to make said policy available to clients and/or consumers upon request and in at least one other format.	CRA must provide a copy of the Consumer Information Privacy Policy along with the address of the policy on the CRA's website (if CRA has website). CRA must provide written policy, procedure, or other documentation explaining other means by which privacy policy is requested and provided.	CRA workers must be able to access current copy of Privacy Policy and access current documentation describing process by which privacy policy is provided externally. CRA must provide evidence of adherence to procedures.	The policy must include, but is not limited to, the following: the purpose of the collection of consumer information, the intended use, and how the information will be shared, stored and destroyed. The CRA must post this policy on its website, if it has one, and have procedure to make said policy available to clients and/or consumers upon request utilizing at least one other method. Auditor will seek evidence of adherence to policies and procedures.
1.10 Unauthorized Browsing			
CRA must have and follow a policy that prohibits CRA workers from searching files and databases unless they have a bona fide business necessity.	CRA must provide written policy, procedure, or other document (CRA worker handbook, etc.) which instructs CRA workers on appropriate and/or inappropriate access and use of consumer information.	CRA workers with access to consumer information must demonstrate knowledge of proper access and use of consumer information and be able to access current copy of documentation. CRA must provide evidence of adherence to procedures.	Documentation must include, but is not limited to, statement of appropriate use as being limited to business purposes only and include prohibition of browsing. Auditor will seek evidence of adherence to policies and procedures.
1.11 Record Destruction			
When records containing consumer information are to be destroyed or disposed of, CRA must have and follow a policy meeting all applicable legal and regulatory requirements and ensure that all such records and data are destroyed and unrecoverable.	CRA must provide written policy, procedure, or other document (CRA worker handbook, etc.) which instructs CRA workers on appropriate document disposal and destruction procedures.	CRA workers must demonstrate knowledge and use of proper document disposal and destruction procedures and be able to access current documentation. CRA must provide evidence of adherence to procedures.	Documentation must require all consumer and client information be destroyed and disposed of securely as to render information inaccessible, unreadable, and unrecoverable. Per current FTC rules (found at 16 CFR Part 682) the following methods are permitted: 1) burning, pulverizing, or shredding, 2) destroying or erasing electronic files, and/or 3) after conducting due diligence, hiring a document destruction company. In addition, paper documents containing personally identifiable information (particularly name, date of birth, and SSN), if retained at individual desks/workstations, must be destroyed or inaccessible no later than the end of each work day/work shift. Auditor will seek evidence of adherence to policies and procedures.
1.12 Sensitive Data Masking			
CRA must have and follow a procedure to suppress or truncate Social Security Numbers and other sensitive data elements as required by law. If end user requires full SSN or other sensitive data elements, CRA must obtain certification from end user that end user will comply with all applicable legal and regulatory requirements in regard to use, safeguarding, and destruction of such information.	CRA must provide written policy, procedure, or other documentation describing suppression, truncation, or other methods used to protect and limit exposure of SSNs and other sensitive data elements as required by law.	CRA workers must demonstrate knowledge of proper procedures for use of SSN's and other sensitive data elements as required by law and CRA workers shall be able to access current documentation. If interviewed, CRA workers must demonstrate understanding of proper use and protection of SSN's and other sensitive data elements as required by law AND if applicable, the use of technology to protect SSN's and other sensitive data elements as required by law. CRA must provide evidence of adherence to	Documentation must include but is not limited to: 1) No more than the final four digits of SSNs shall be communicated in any form outside the CRA environment unless an approved exception exists; 2) When use of SSN and other sensitive data elements as required by law is needed internally or externally, the data exposed shall be limited to only that which is needed for the specific business purpose which has been identified; 3) When communicating SSNs or other data elements as required by law or necessary business purpose outside the CRA environment, secure transport methods must be used. Auditor will seek evidence of adherence to policies and procedures.

NAPBS BACKGROUND SCREENING AGENCY ACCREDITATION PROGRAM (BSAAP) – ACCREDITATION STANDARD AND AUDIT CRITERIA

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)
		procedures.	
Legal and Compliance			
2.1 Compliance with Law and Regulation			
The CRA must comply with all provisions of all applicable law and regulation pertaining to the consumer reports provided by the CRA for employment purposes. This includes, but is not limited to, the Federal FCRA and all legal and regulatory requirements identified in this Accreditation Standard.	CRA must provide written policy, procedure, or other documentation which clearly informs CRA workers of requirement to comply with all applicable law and regulation including, but not limited to, the FCRA and all legal and regulatory requirements identified in this Accreditation Standard.	CRA workers must demonstrate knowledge of compliance requirement and be able to access current copy of documentation. CRA workers must be able to identify person/s responsible for legal and regulatory compliance. CRA must provide evidence of adherence to procedures.	CRA must provide documentation describing how CRA workers are informed of compliance requirement and compliance leader/s. Methods to inform CRA workers must include at least one of the following: 1) inclusion in CRA Worker Handbook, 2) inclusion in CRA worker employment agreement, or 3) inclusion in online document repository where CRA operational policies and procedures are made available to employees. Auditor will seek evidence of adherence to policies and procedures.
2.2 Federal Consumer Reporting Law			
The CRA must designate an individual(s) or position(s) within the organization responsible for CRA's compliance with all sections of the federal FCRA that pertain to the consumer reports provided by the CRA for employment purposes.	CRA must employ a minimum of one person who is responsible for CRA's development, implementation, and on-going compliance with all applicable sections of the FCRA as evidenced by written job description/s or other documentation. If multiple people are responsible, one person must hold overall responsibility as evidenced by written job description or other documentation. Compliance leader must hold current NAPBS Advanced FCRA Certificate OR Juris Doctorate and CRA must provide evidence of the same.	CRA must present written job description, policy, procedure or other documentation which identifies, by name and/or title, the person responsible for FCRA compliance. Compliance Leader must hold current NAPBS Advanced FCRA Certificate or Juris Doctorate and CRA must provide evidence of the same. CRA must make this person available in person. If interviewed, CRA workers must identify the person(s) that can provide FCRA expertise when needed.	CRA Compliance Leader must affirm his/her role as being responsible for FCRA compliance within the organization.
2.3 State Consumer Reporting Law			
The CRA must designate an individual(s) or position(s) within the organization responsible for compliance with all state consumer reporting laws that pertain to the consumer reports provided by the CRA for employment purposes.	CRA must employ a minimum of one person who is responsible for CRA's development, implementation, and on-going compliance with all applicable state consumer-reporting law as evidenced by written job description/s or other documentation. If multiple people are responsible, one person must hold overall responsibility as evidenced by written job description or other documentation. Compliance leader must hold current NAPBS Advanced FCRA Certificate OR Juris Doctorate and CRA must provide evidence of the same.	CRA must present written job description, policy, procedure or other documentation which identifies, by name and/or title, the person responsible for state consumer reporting law compliance. Compliance Leader must hold current NAPBS Advanced FCRA Certificate or Juris Doctorate and CRA must provide evidence of the same. CRA must make this person available in person. If interviewed, CRA workers must identify the person(s) that can provide state consumer reporting law expertise when needed.	CRA Compliance Leader must affirm his/her role as being responsible for state consumer reporting law compliance within the organization.
2.4 Driver Privacy Protection Act (DPPA)			
The CRA must designate an individual(s) or position(s) within the organization responsible for compliance with the DPPA that pertain to the consumer reports provided by the CRA for employment purposes, if the CRA furnishes consumer reports that contain information subject to the DPPA.	CRA must employ a minimum of one person who is responsible for CRA's development, implementation, and on-going compliance with all applicable DPPA law as evidenced by written job description/s or other documentation. If multiple people are responsible, one person must hold overall responsibility as evidenced by	CRA must present written job description, policy, procedure or other documentation which identifies, by name and/or title, the person responsible for DPPA compliance. CRA must make this person available either in person, by phone **OR** shall provide a signed affidavit. If interviewed, CRA workers must identify the person(s) that can provide DPPA expertise when	CRA Compliance Leader must affirm his/her role as being responsible for DPPA compliance within the organization.

NAPBS BACKGROUND SCREENING AGENCY ACCREDITATION PROGRAM (BSAAP) – ACCREDITATION STANDARD AND AUDIT CRITERIA

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)
	written job description or other documentation.	needed.	
2.5 State Implemented DPPA Compliance			
The CRA must designate an individual(s) or position(s) within the organization responsible for compliance with state implementations of the DPPA that pertain to the consumer reports provided by the CRA for employment purposes, if the CRA furnishes consumer reports that contain information subject to state implementations of the DPPA.	CRA must employ a minimum of one person who is responsible for CRA's development, implementation, and on-going compliance with all applicable state DPPA laws as evidenced by written job description/s or other documentation. If multiple people are responsible, one person must hold overall responsibility as evidenced by written job description or other documentation.	CRA must present written job description, policy, procedure or other documentation which identifies, by name and/or title, the person responsible for state DPPA law compliance. CRA must make this person available either in person, by phone **OR** shall provide a signed affidavit. If interviewed, CRA workers shall identify the person/s that can provide state DPPA expertise when needed.	CRA Compliance Leader must affirm his/her role as being responsible for state DPPA law compliance within the organization.
2.6 Integrity			
CRA must have and follow a policy of not engaging in bribery or any other fraudulent activity to obtain preferential treatment from a public official or government entity.	CRA must provide written policy, procedure, or other written documentation (such as CRA worker handbook) clearly prohibiting bribery or any other fraudulent activity to obtain preferential treatment from a public official or government entity.	CRA must present one or more documents which clearly prohibit bribery or any other fraudulent activity to obtain preferential treatment from a public official or government entity. If interviewed, CRA workers responsible for obtaining public record information must demonstrate knowledge of anti-bribery/fraudulent activity policy and be able to access current documentation. CRA must affirm that they do not engage in bribery or other fraudulent activity and that CRA has never been convicted of such activity.	The policy must include, but is not limited to, prohibition of bribery and any other fraudulent activity. If CRA has been convicted of bribery or other fraudulent activity, auditor must advise Background Screening Credentialing Council (BSCC). BSCC must review specifics of case to determine whether CRA may proceed with the accreditation process.
2.7 Prescribed Notices			
CRA must have and follow a procedure to provide client current version of all currently required federal notices required by the FCRA, such as those prescribed by the CFPB.	CRA must provide written policy, procedure, or other written documentation describing when/how clients are provided with copies of required CFPB publications.	CRA must present one or more documents which provide evidence that CRA provides prescribed documents to client. CRA must make available the person responsible for providing notices either in person or by phone. CRA must provide evidence of adherence to procedures.	CRA must provide documentation describing how required notices are provided to clients. Methods include, but are not limited to providing as part of a Client agreement, User agreement or some other document. Per the FCRA, such notices currently include: 1) Notice to Users of Consumer Reports: Obligations of Users under the FCRA, and 2) A Summary of Your Rights Under the Fair Credit Reporting Act. Auditor will seek evidence of adherence to policies and procedures.
2.8 Agreement from Client			
Before providing consumer reports to clients, CRA must have and follow a procedure to obtain a signed agreement, certification, affirmation or other signed document from client (referred to as "user" in federal FCRA) in which client agrees to	CRA must provide written policy, procedure, or other written documentation describing when and how clients sign required agreement, certification, affirmation, or other document in which client agrees to comply with all	CRA must present written procedure for obtaining signed agreement, certification, affirmation, or other document, copy of signed agreement, and demonstrate where/how signed agreements are	CRA must provide documentation describing how signed agreements, certifications, affirmations, or other documents are obtained and retained. The agreement must meet requirements of federal FCRA, which currently include: 1) permissible purpose, 2) disclosure and authorization, 3) adverse action, 4) confidentiality, 5) compliance with all applicable laws

NAPBS BACKGROUND SCREENING AGENCY ACCREDITATION PROGRAM (BSAAP) – ACCREDITATION STANDARD AND AUDIT CRITERIA

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)
meet the requirements of all applicable law and regulation, specifically including but not limited to the federal FCRA.	applicable law and regulation, specifically including but not limited to the FCRA, and where such agreements are retained. CRA must also provide copy of such agreement.	retained. CRA must make available the person responsible for retaining these agreements and auditor may ask to see (but not retain a copy of) signed agreements from one or more clients. CRA workers responsible for activating client access to CRA systems/products must demonstrate knowledge that pre-requisites exist before client is permitted access to CRA's products/ systems and how the CRA worker knows it is permissible to activate access. CRA must provide evidence of adherence to procedures.	and regulations, 6) that client will not use consumer information in violation of law. Auditor will seek evidence of adherence to policies and procedures.
2.9 Client Legal Responsibilities			
CRA must have and follow procedures to inform client that client has legal responsibilities when procuring and using consumer reports for employment purposes. CRA must recommend to client that client work with legal counsel to ensure compliance with their specific legal responsibilities.	CRA must provide written policy, procedure, or other documentation describing how/when clients are informed that client has legal responsibilities when procuring and using consumer reports for employment purposes and when/how CRA informs clients of necessity of consulting with their legal counsel regarding client's specific legal responsibilities.	CRA must present written procedure for informing client that client has legal responsibilities and advising client to consult with legal counsel. CRA must make available the document/s used to so inform clients, the person responsible for retaining signed acknowledgments, and auditor may ask to see (but not retain a copy of) signed acknowledgments from one or more clients. CRA must provide evidence of adherence to procedures.	CRA must: 1) inform clients that client has legal responsibilities, and 2) advise client to consult with legal counsel. Methods include but are not limited to Client agreement, User agreement, or some other document which is signed by the client and includes, but is not limited to, client acknowledgement of legal responsibilities. Per the FCRA, current legal responsibilities include: 1) having permissible purpose, 2) disclosing to consumer, 3) obtaining consumer 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. Auditor will seek evidence of adherence to policies and procedures.
2.10 Client Required Documents			
CRA must have and follow procedures to inform client of specific forms or documents required to complete specific searches.	CRA must provide written policy, procedure, or other documentation describing how/when clients are informed of specific forms or documents which are required for completion of a search the client has requested.	CRA must present written procedure describing how/when clients are informed of specific forms or documents that are necessary in order to complete one or more of the searches requested by the client. CRA must make available person responsible for informing clients of specific forms or documents required to complete specific searches, and auditor may ask to see (but not retain a copy of) completed forms or documents. CRA must provide evidence of adherence to procedures.	CRA must have and follow procedures to inform client of specific forms or documents required to complete specific searches. Auditor will seek evidence of adherence to policies and procedures.
2.11 Disclosure and Authorization			
CRA must have and follow a procedure to inform client of legal requirements imposed by the federal FCRA and, in some instances, state consumer reporting laws, regarding disclosing to and obtaining authorization from consumers prior to requesting a consumer report from CRA. CRA must recommend to client that client consult with counsel to develop a legally compliant disclosure and authorization process.	CRA must provide written policy, procedure, or other documentation describing how/when clients are informed of legal requirements imposed by the federal FCRA and, in some instances, state consumer reporting laws, regarding providing disclosure to and obtaining authorization from consumer prior to requesting a consumer report from CRA. CRA must also provide copy of document used to recommend to client that client consult with counsel to develop legally	CRA must present written procedure for informing client of legal requirements regarding disclosure and authorization and advising client to consult with legal counsel. CRA must make available the document(s) used to so inform clients, the person responsible for retaining signed acknowledgments, and auditor may ask to see (but not retain a copy of) signed acknowledgments from one or more clients. If interviewed, CRA workers must demonstrate	CRA must inform client of legal requirements regarding disclosure and authorization. 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 client acknowledgement. Per the FCRA, client's current legal responsibilities include providing proper disclosure and obtaining written authorization before requesting consumer report from CRA. Auditor will seek evidence of adherence to policies and procedures.

NAPBS BACKGROUND SCREENING AGENCY ACCREDITATION PROGRAM (BSAAP) – ACCREDITATION STANDARD AND AUDIT CRITERIA

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)
	compliant disclosure and authorization policy and procedures.	knowledge of client's requirement to follow disclosure and authorization processes, be able to access current copy of documentation; and/or workers must identify person/s to address such topics. CRA must provide evidence of adherence to procedures.	
2.12 Adverse Action			
CRA must have and follow a procedure to inform client of legal requirements imposed by the federal FCRA and, in some instances, state consumer reporting laws, regarding taking adverse action against a consumer based on a consumer report. CRA must recommend to client that client consult with counsel to develop a legally compliant adverse action process.	CRA must provide written policy, procedure, or other documentation describing how/when clients are informed of legal requirements imposed by the federal FCRA and, in some instances, state consumer reporting laws, regarding taking adverse action against a consumer based on a consumer report. CRA must also provide copy of document used to recommend to client that client consult with counsel to develop legally compliant adverse action policy and procedures.	CRA must present written procedure for informing client of legal requirements regarding adverse action and advising client to consult with legal counsel. CRA must make available the document/s used to so inform clients, the person responsible for retaining signed acknowledgments, and auditor may ask to see (but not retain a copy of) signed acknowledgments from one or more clients. If interviewed, CRA workers must demonstrate knowledge of client's requirement to follow adverse action processes, be able to access current copy of documentation; AND/OR CRA workers shall identify person/s to address such topics. CRA must provide evidence of adherence to procedures.	CRA must inform client of legal requirements regarding adverse action. 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 client acknowledgement. Per the FCRA, client's current legal responsibilities regarding adverse action must include: 1) providing pre-adverse action notice to consumer, along with copy of consumer report and "A Summary of Your Rights Under the Fair Credit Reporting Act," 2) allowing consumer a designated period of time to contact CRA if consumer wishes to dispute any information in consumer report, 3) providing CRA contact information, 4) providing a final adverse action notice to consumer if a final adverse employment decision is made. Auditor will seek evidence of adherence to policies and procedures.
2.13 Consumer Disputes			
CRA must have and follow procedures for handling and documenting a consumer dispute. At a minimum, procedures must meet all applicable legal and regulatory requirements.	CRA must provide written policy, procedure, or other documentation which instructs CRA workers on consumer dispute procedures.	CRA workers responsible for consumer disputes must demonstrate knowledge of proper consumer dispute procedures and be able to access current copy of documentation. Auditor may request to see a copy of dispute documentation and redacted examples of consumer dispute processing. CRA must provide evidence of adherence to procedures.	The policies and procedures designed to handle consumer disputes must meet FCRA requirements which include, but are not limited to: 1) no charge to consumer; 2) re-investigate, correct, and/or delete disputed information within 30 days (or 45 days if extended) of notice of dispute; 3) notify furnisher of information of dispute within 5 business days of receipt; 4) in the case of a reseller, notify each consumer reporting agency having provided information to reseller, 5) consider information provided by consumer, 6) advise consumer if dispute is deemed frivolous or irrelevant 7) notify appropriate parties of dispute results, and 8) comply with consumer request for description of re-investigation process. In addition, CRA must document: 1) responsibility of CRA employee receiving consumer dispute, 2) how incoming consumer dispute letters/emails/phone calls must be routed upon receipt, 3) re-investigation responsibility and/or procedures, 4) process for updating/correcting consumer report, 5) recordkeeping, and 6) procedure to help prevent future occurrences (such as recommendation for training, software change, etc.). Auditor will seek evidence of adherence to policies and procedures.
2.14 Database Criminal Records			
When reporting public record information which is likely to have an adverse effect on a consumer's ability to obtain employment, pursuant to the federal FCRA the CRA shall either: A) maintain strict procedures designed to insure the reported information is complete and up to date; or B) at the time such public record information is reported to the user of such consumer report, notify the consumer of the fact that public record information is being reported by the CRA, together with the name and address	CRA shall provide written policy, procedure, or other documentation describing method/s used to comply with current FCRA requirements of maintaining procedures designed to insure information is complete and up to date prior to reporting, or providing notice to the consumer at the time information is reported to user of the consumer report.	CRA employees responsible for reporting public record information which is likely to have an adverse effect on a consumer's ability to obtain employment shall demonstrate knowledge of procedures and be able to access current documentation.	The policy/procedure should include either: 1) process used to ensure the reported information is complete and up to date, or 2) process used to notify consumer of the fact that potentially adverse public record information is being reported to the user of the consumer report.

NAPBS BACKGROUND SCREENING AGENCY ACCREDITATION PROGRAM (BSAAP) – ACCREDITATION STANDARD AND AUDIT CRITERIA

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)
of the person to whom such information is being reported.			
2.15 Identification Confirmation			
CRA must have and follow procedures requiring reasonable procedures to assure maximum possible accuracy when determining the identity of a consumer who is the subject of a record prior to reporting the information.	CRA must provide written policy, procedure, or other written documentation describing reasonable procedures used to assure maximum possible accuracy when determining the identity of a consumer who is the subject of a record prior to reporting the information.	CRA must present written reasonable procedures to assure maximum possible accuracy when determining the identity of a consumer who is the subject of a record prior to reporting the information. CRA shall make available the person responsible for ensuring compliance with CRA's policy in regard to assuring maximum possible accuracy. CRA workers responsible for such identification must demonstrate knowledge of identification requirement and be able to access current documentation. CRA must provide evidence of adherence to procedures.	Reasonable procedures to assure maximum possible accuracy must include, but are not limited to: 1) matching a minimum of two identifiers where one identifier is first name + middle name/middle initial where available + last name (or reasonable derivative thereof); and second identifier is: a) month of birth + day of birth + year of birth, b) SSN, c) driver's license number, d) passport or country identification number, e) current or previous addresses, or f) multiple partial identifiers; **OR** 2)Any reasonable procedures that are demonstrably as effective as those described in 1. Auditor will seek evidence of adherence to policies and procedures.
2.16 Full File Disclosure			
CRA must have and follow procedures for documenting and responding to a consumer request for all information in consumer's file.	CRA must provide written policy, procedure, or other documentation which: 1) instructs CRA workers on procedures to comply with consumer request for all information in consumer's file, and 2) describes how records of such requests and responses are created and maintained.	CRA workers responsible for responding to consumer request for all information in consumer's file must demonstrate knowledge of proper procedures and be able to access current copy of documentation. CRA must make available the person responsible for ensuring compliance with CRA's policy in regard to providing all information in consumer's file. CRA workers responsible for providing such information must demonstrate knowledge of requirement and be able to access current documentation. CRA must provide evidence of adherence to procedures.	The policies and procedures designed to handle consumer requests for all information in consumer's file must meet Federal FCRA requirements including the requirement for CRA to obtain proper identification from the consumer. For CRAs preparing consumer reports only for employment purposes, information to be provided must include, but is not limited to, all information in consumer's file at time of request including: 1) Identification of each person procuring a consumer report for employment purposes about consumer for the 2-year period preceding consumer request and 2) source information except those acquired and used solely in preparing an investigative consumer report. Policies and procedures must include how records of consumer requests and CRAs responses are created and maintained. Auditor will seek evidence of adherence to policies and procedures.
2.17 Jurisdictional Knowledge			
The CRA must employ or have access to a qualified individual(s) within the organization or through a designated service provider, who is responsible for understanding court terminology, as well as understanding the various jurisdictional court differences if CRA reports court records.	CRA must employ or have access to a qualified individual(s) within the organization or through a designated service provider, who is responsible for understanding, court terminology, as well as understanding the various jurisdictional court differences if CRA reports court records. If multiple people are responsible, one person must hold overall responsibility as evidenced by written job description or other documentation.	CRA must present written job description, policy, procedure or other documentation which identifies, by name and/or title, the person responsible for court/jurisdictional knowledge. If a vendor is used to support this requirement, the vendor's evidence must be provided. CRA must make this person available in person, by phone, or CRA shall provide signed affidavit. If interviewed, this individual shall demonstrate knowledge of court and jurisdictional knowledge as well as identifying resources for additional information. If interviewed, CRA workers shall identify the person(s) who can provide court/jurisdictional expertise when needed.	To be qualified, the individual must have one or more of the following: 1) criminal justice degree, 2) law enforcement experience, 3) legal experience, 4) court experience, 5) investigator experience, and/or 6) three years' work experience with court records. If a vendor is used to fulfill this requirement, evidence must be provided to support the vendor-CRA relationship and confirmation that the vendor supports the CRA with this knowledge requirement.
2.18 Automated Reporting Systems			
If CRA uses automated reporting systems, CRA must have and	CRA must provide written policy, procedure, or other	CRA must present procedures to monitor accuracy of	Procedures for auditing automated reporting systems must include, but are not limited to: 1)

NAPBS BACKGROUND SCREENING AGENCY ACCREDITATION PROGRAM (BSAAP) – ACCREDITATION STANDARD AND AUDIT CRITERIA

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)
follow reasonable procedures to ensure results as reported on consumer report accurately reflect source information received into the automated reporting system.	documentation defining methods used to monitor accuracy of automated reporting systems.	automated reporting system results and take corrective actions when necessary. CRA shall make available to auditor tools or systems used. If interviewed, CRA workers responsible for automated reporting systems must demonstrate knowledge of methods, must be able to access current copy of documentation, and must identify person(s) responsible for providing on-the-job automated reporting leadership. CRA must provide evidence of adherence to procedures.	results as reported on consumer report accurately reflect source information received into the automated reporting system, 2) quantifying quality lapses, if any, 3) analyzing nature of lapses if any, 4) conducting root cause analysis, if any, and 5) developing and implementing appropriate corrective actions, if any. Procedures must include retention of monitoring records. Auditor will seek evidence of adherence to policies and procedures.
2.19 Quality			
CRA must have and follow procedures to reasonably ensure the accuracy and quality of all work product. CRA must have and follow accuracy and quality procedures specific to work product containing public records likely to have an adverse effect on consumer. The CRA must take into account the particular nature of public records research and reporting when designing and implementing the specific procedures related to accuracy, completeness, and currency of public records research and reporting likely to have an adverse effect on consumers. CRA must designate an individual(s) or position(s) within the organization responsible for quality.	CRA must provide written policy, procedure, or other documentation describing the procedures used to reasonably ensure the accuracy and quality of all work product, and procedures specific to work product containing public records likely to have an adverse effect on consumer.	CRA must present procedures which are in place to reasonably ensure the accuracy and quality of all work-product, and procedures specific to work product containing public records likely to have an adverse effect on consumer. CRA shall make available to auditor tools or systems used (except actual personally identifiable information) to reasonably ensure accuracy and quality in all work product. If interviewed, CRA workers responsible for work product must demonstrate knowledge of accuracy and quality requirements, describe methods used to ensure quality and accuracy, must be able to access current copy of documentation, and must identify person/s responsible for providing on-the-job quality and accuracy leadership. CRA must provide evidence of adherence to procedures.	CRA must provide information regarding quality and accuracy of work product to CRA workers who are responsible for such quality and accuracy by using various methods which include, but are not limited to: 1) written manuals, 2) online manuals or instructions, 3) classroom training, 4) on-the-job training, and/or availability of expert to provide assistance when needed. If classroom or on-the-job training is used, a training outline or manual must be used. Auditor will seek evidence of adherence to policies and procedures.
	CRA must employ a minimum of one person who is responsible for CRA's quality as evidenced by written job description/s or other documentation. If multiple people are responsible, one person must hold overall responsibility as evidenced by written job description or other documentation.	CRA must present written job description, policy, procedure or other documentation which identifies, by name and/or title, the person responsible for quality. CRA must make this person available either in person or by phone. If interviewed, CRA workers must identify the person/s responsible for quality.	CRA quality leader must affirm his/her role as being responsible for quality within the organization.
2.20 Reappearance of Inaccurate Information			
CRA must have and follow procedures to prevent reappearance of inaccurate consumer information in consumer reports.	CRA must provide written policy, procedure, or other written documentation describing procedures used to prevent reappearance of inaccurate consumer information in consumer reports.	CRA must present written documentation for preventing reappearance of inaccurate consumer information in consumer reports. CRA must make available the person responsible for ensuring compliance with CRA's policy in regard to preventing reappearance of inaccurate consumer information. CRA workers responsible for such prevention must demonstrate knowledge of prevention requirement and be able to access current documentation. CRA must provide evidence of adherence to procedures.	Procedures must include process by which re-reporting of inaccurate information is prevented. Recommended procedures must include, but are not limited to: 1) identifying consumers who previously had inaccurate information reported, who disputed such information, and for whom CRA removed or otherwise corrected inaccurate information, and 2) method/s by which previously reported inaccurate information is prevented from being included in new reports. Auditor will seek evidence of adherence to policies and procedures.

NAPBS BACKGROUND SCREENING AGENCY ACCREDITATION PROGRAM (BSAAP) – ACCREDITATION STANDARD AND AUDIT CRITERIA

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)
2.21 Quality Analysis			
CRA must have and follow procedures to audit and analyze product quality. Identified quality lapses, including those identified during consumer disputes, must be quantified and analyzed, including root cause analysis, and appropriate corrective actions must be implemented.	CRA must provide written policy, procedure, or other documentation describing the methods used to quantify and analyze quality failures, including root cause analysis, and implement appropriate corrective actions. Procedures must include two types of quality testing: 1) work product initially free of defect, and 2) work product containing quality failures (whether identified internally or through consumer dispute).	CRA must present written documentation to quantify and analyze quality lapses, including root cause analysis, and implement appropriate corrective actions. CRA shall make available to auditor tools or systems used (except actual personally identifiable information). If interviewed, CRA workers responsible for quality analysis must demonstrate knowledge of methods, must be able to access current copy of documentation, and must identify person(s) responsible for providing on-the-job quality analysis leadership. CRA must provide evidence of adherence to procedures.	Procedures for quality control and analysis must include, but are not limited to: 1) an established protocol for systematically sampling results provided in consumer report, 2) quantifying quality lapses, 3) analyzing nature of lapses, 4) process for conducting root cause analysis, and 5) developing and implementing appropriate corrective actions. Procedures must include retention of monitoring records. Auditor will seek evidence of adherence to policies and procedures.
Client Education			
3.1 Truth in Advertising			
CRA must have and follow a procedure to communicate to clients the original source type (county records, state records, employer, academic institution, etc.), limitations, variables affecting the information available and scope of information provided by each consumer reporting product offered by the CRA.	CRA must provide written policy, procedure, or other documentation describing how/when clients are provided with information that describes the composition of each consumer reporting product, type of information source(s) used for each consumer reporting product, factors affecting the information, and any parameters or conditions applied by the CRA when reporting to client. CRA must provide copy of documents used to so inform clients. If CRA provides actual consumer reports to demonstrate full and accurate consumer reporting product disclosure, all personally identified information must be redacted.	CRA must present written procedure for providing information to clients that accurately describes consumer reporting products, including one or more samples of provided documents. If consumer reports are used to demonstrate full and accurate consumer reporting product disclosure, all personally identified information must be redacted and auditor will not retain copy. If interviewed, CRA workers must demonstrate knowledge that consumer reporting product descriptions exist, where such descriptions are retained, and/or the person responsible for CRA's consumer-reporting products. CRA must provide evidence of adherence to procedures.	CRA must inform clients of specific composition of consumer reporting products. Information disclosed regarding consumer reporting products must include, but is not limited to: 1) type of source, 2) scope of records searched, 3) and search methodology. It is recommended that disclosure of information source, type of source, scope of search, and search methodology be included in consumer reports. Lacking such disclosure, reports should explain how user of consumer report may obtain such information. Auditor will seek evidence of adherence to policies and procedures.
3.2 Legal Counsel			
CRA must have and follow a procedure to inform client that CRA is not acting as legal counsel and cannot provide legal advice. CRA must inform client of the importance of working with counsel to develop an employment screening program specific to their needs and to ensure that client's policies and procedures related to the use of CRA-provided information are in compliance with all applicable legal and regulatory requirements.	CRA must provide written policy, procedure, or other documentation describing how/when clients are informed that CRA is not acting as legal counsel and cannot provide legal advice. CRA must provide copy of document used to so inform client and such document must include advising client to work with legal counsel regarding client's specific screening program, policies, and procedures to ensure legal compliance.	CRA must present written procedure for informing client that CRA does not provide legal advice or act as client's legal counsel. CRA must make available the document/s used to so inform clients, the person responsible for retaining signed acknowledgments, and auditor may ask to see (but not retain a copy of) signed acknowledgments from one or more clients. If interviewed, CRA workers must demonstrate knowledge of CRA's position that legal counsel is not	CRA must inform clients that CRA does not function as legal counsel. 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 client acknowledgement. Such acknowledgment must include, but is not limited to: 1) CRA is not legal counsel and does not provide legal advice, 2) advising client of importance of working with their legal counsel to ensure overall screening program compliance, and 3) advising clients that consumer reports provided by CRA must be used in compliance with all applicable legal and regulatory requirements. Auditor will seek evidence of adherence to policies and procedures.

NAPBS BACKGROUND SCREENING AGENCY ACCREDITATION PROGRAM (BSAAP) – ACCREDITATION STANDARD AND AUDIT CRITERIA

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)
		provided, be able to access current copy of documentation, and/or CRA workers must identify person(s) to address legal topics. CRA must provide evidence of adherence to procedures.	
3.3 Understanding Consumer Reports			
CRA must have and follow a procedure to provide guidance to client on how to order, retrieve, read and understand the information provided in consumer reports provided by the CRA.	CRA must provide written policy, procedure, or other documentation describing how/when clients are provided with information regarding obtaining and understanding consumer reports. CRA must provide copy of document/s used to so inform client, must demonstrate online tools/information (such as User Guide or online Help) provided to clients, or other method/s used to assist clients.	CRA must present written procedure for informing client how to obtain and understand consumer reports from CRA. CRA must make available the documents or systems used to so inform clients. If interviewed, CRA workers must demonstrate knowledge of how such education is provided, be able to access current copy of documentation, and/or CRA workers shall identify person/s to address such topics. CRA must provide evidence of adherence to procedures.	CRA must provide information to clients regarding how to order, retrieve, read, and understand consumer reports by using one or more methods which include, but are not limited to: 1) user manual/guide, 2) online training, user guides, or help system, 3) user training classes/webinars, 4) one-on-one training sessions, or 5) verbal assistance. Auditor will seek evidence of adherence to policies and procedures.
3.4 Information Protection			
CRA must have and follow a procedure to inform client of: 1) the sensitive nature of consumer reports, 2) the requirement to protect such information, and 3) the consumer report retention and destruction practices as outlined in the federal FCRA and the DPPA.	CRA must provide written policy, procedure, or other documentation describing how/when clients are informed regarding the importance of and legal requirement to protect consumer data presented in consumer reports. CRA must provide copy of document/s used to so inform client.	CRA must present written procedure for informing client of client's legal responsibilities regarding protection of consumer data. CRA must present the document/s used to so inform clients, the person responsible for retaining signed acknowledgments, and auditor may ask to see (but not retain a copy of) signed acknowledgments from one or more clients. If interviewed, CRA workers must demonstrate knowledge of client's requirement to protect consumer data, be able to access current copy of documentation; and/or CRA workers shall identify person(s) to address such topics. CRA must provide evidence of adherence to procedures.	CRA must inform clients of client's legal requirements regarding protection of consumer data. 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 consumer data protection responsibilities. Per the FCRA, current requirements include: 1) limiting dissemination of consumer information to only those with legitimate need, permissible purpose, and authorized by consumer; 2) retaining consumer data in a confidential manner; and 3) destroying data in a secure manner as specified in current FTC document destruction rules. Per the DPPA, current requirements include: 1) protecting the privacy of consumer information which is contained in motor vehicle records and, 2) accessing DMV records only with written consent of consumer. Auditor will seek evidence of adherence to policies and procedures.
Researcher and Data Standards			
4.1 Public Record Researcher Agreement			
CRA must have and follow a procedure requiring a signed agreement, which may include amendments and/or addenda, from all non-employee public record researchers. The agreement must clearly define the scope of services to be	CRA must provide written policy, procedure, or other written documentation describing how a signed agreement covering scope of services is obtained from and retained for all current public record researchers.	CRA must present written procedure for obtaining signed agreement, copy of agreement, and demonstrate where/how signed agreements are retained. CRA must make available the person	The agreement must include, but is not limited to: 1) the requirement to conduct all searches in full compliance with applicable law and regulation, 2) jurisdictions covered, 3) search methodology, 4) depth of search, 5) disclosure of findings, 6) methodology and time frame for communication and completion of requests, 7) methodology for confirming identity of subject

NAPBS BACKGROUND SCREENING AGENCY ACCREDITATION PROGRAM (BSAAP) – ACCREDITATION STANDARD AND AUDIT CRITERIA

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)
provided, including jurisdictions covered, search methodology, depth of search, disclosure of findings, methodology and time frame for communication and completion of requests, methodology for confirming identity of subject of record(s), confidentiality requirements, reinvestigation requirements, and other obligations as furnishers of information under the federal FCRA.	CRA must also provide copy of current agreement. (Note: This agreement may also incorporate Certification requirements of Clause 4.3.)	responsible for obtaining and retaining these agreements and auditor may ask to see (but not retain a copy of) signed agreements from one or more public record researchers. If interviewed, CRA workers responsible for working with public record researchers must demonstrate understanding of requirement for signed agreement prior to utilizing services of public record researcher OR technology must prevent utilization of public record researcher by CRA workers until CRA Leader has enabled use. CRA must provide evidence of adherence to procedures.	of record(s), 8) confidentiality requirements, 9) reinvestigation requirements, 10) other obligations as a furnisher of information under the federal FCRA, and 11) the requirement for public record researcher to obtain a similar agreement from subcontractors, if subcontractors are used. In particular, the agreement must emphasize confidentiality requirements including: 1) the legal requirement to treat all consumer information as confidential, 2) secure data transmission, and 3) secure and timely disposal of confidential information. (Note: This agreement may incorporate the Certification requirement of Clause 4.3) Auditor will seek evidence of adherence to policies and procedures.
4.2 Vetting Requirement			
CRA must have and follow procedures to vet new public record researchers.	CRA must provide written policy, procedure, or other written documentation describing the requirement to and methodology used to vet new public record researchers.	CRA must present written procedure for vetting new public record researchers, and demonstrate where/how records are retained. CRA shall make available the person responsible for such vetting and auditor may ask to see (but not retain a copy of) vetting records from one or more public record researchers. If interviewed, CRA workers responsible for working with public record researchers must demonstrate understanding of vetting requirement prior to utilizing services of public record researcher OR technology must prevent utilization of public record researcher by CRA workers until CRA Leader has enabled use. CRA must provide evidence of adherence to procedures.	The vetting records must include, but are not limited to: 1) evidence of right to conduct business, such as copy of business license, articles of incorporation, state filing etc., and authentication thereof, 2) verification of required private investigator license, if such license is required and 3) results of test searches conducted. The vetting records may include, but are not limited to: 1) completed favorable reference interviews from at least one current client, 2) verification of association memberships such as local Chamber of Commerce, Better Business Bureau, NCISS, ASIS, and/or NAPBS and3) confirmation of certificate received by successfully completing the "NAPBS RESEARCH PROVIDER EXAMINATION." Auditor will seek evidence of adherence to policies and procedures.
4.3 Public Record Researcher Certification			
CRA must have and follow a procedure requiring public record researcher to certify in writing that they will conduct research in compliance with all applicable legal and regulatory requirements, as well as in the manner prescribed by the repository which maintains the official record of the court; never obtain information through illegal or unethical means; and utilize document disposal and/or destruction methods pursuant to the federal FCRA.	CRA must provide written policy, procedure, or other written documentation describing how/when/where the signed certification is obtained from and retained for all current public record researchers. CRA shall also provide copy of current certification. (Note: This certification may be incorporated in or an appendix to the "Public Record Researcher Agreement" described in Clause 4.1.)	CRA must present written procedure for obtaining signed certification, copy of certification, and demonstrate where/how signed certifications are retained. CRA must make available the person responsible for retaining these certifications and auditor may ask to see (but not retain a copy of) signed certifications from one or more public record researchers. (Note: This certification may be part of the "Public Record Researcher Agreement" described in Clause 4.1.) If interviewed, CRA workers responsible for working with public record researchers	The Certification signed by the Public Record Researcher must include, but is not limited to, the following: 1) to comply with all applicable legal and regulatory requirements, as well as in the manner prescribed by the repository which maintains the official record of the court; 2) to obtain information only through legal and ethical means; 3) to dispose of or destroy confidential documents in a secure manner per FTC document destruction rule; 4) to transmit all consumer information in a secure manner; and 5) to allow CRA to audit records. (Note: This certification may be part of the "Public Record Researcher Agreement" described in Clause 4.1.) Auditor will seek evidence of adherence to policies and procedures.

NAPBS BACKGROUND SCREENING AGENCY ACCREDITATION PROGRAM (BSAAP) – ACCREDITATION STANDARD AND AUDIT CRITERIA

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)
		must demonstrate understanding of certification requirement prior to utilizing services of public record researcher or technology must prevent utilization of public record researcher by CRA workers until CRA Leader has enabled use. CRA must provide evidence of adherence to procedures.	
4.4 Errors and Omissions Coverage (E&O)			
CRA must have and follow a procedure to obtain proof of public record researcher's Errors and Omissions Insurance. If public record researcher is unable to provide proof of insurance, CRA must maintain coverage for uninsured and/or underinsured public record researcher.	CRA must provide written policy, procedure, or other written documentation describing the requirement to and method used to verify public record researcher's Errors and Omissions insurance and that such insurance remains in force. If researcher does not have or cannot prove existing coverage, CRA shall provide copy of CRA's insurance policy which contains E&O coverage for uninsured/underinsured public record researchers.	CRA must present written procedure for obtaining proof of public record researcher's E&O insurance and demonstrate where/how such proof documentation is retained. CRA must make available the person responsible for retaining this proof and auditor may ask to see (but not retain a copy of) such proof from one or more public record researchers. In addition, auditor may ask to see (but not retain copy of) CRA's E&O insurance policy in which coverage for uninsured/ underinsured public record researchers is provided. If interviewed, CRA workers responsible for working with public record researchers must demonstrate understanding of E&O insurance requirement prior to utilizing services of public record researcher OR technology must prevent utilization of public record researcher by CRA workers until CRA Leader has enabled use. CRA must provide evidence of adherence to procedures.	Public record researcher E&O insurance must be in force or CRA's E&O insurance must cover CRA public record researchers. A minimum of one million in coverage is required. Auditor will seek evidence of adherence to policies and procedures.
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 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 encrypted or protected in a comparable manner. Auditor will seek evidence of

NAPBS BACKGROUND SCREENING AGENCY ACCREDITATION PROGRAM (BSAAP) – ACCREDITATION STANDARD AND AUDIT CRITERIA

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)
			adherence to policies and procedures.
4.6 Auditing Procedures			
CRA must have and follow a procedure to audit their active public record researchers for quality.	CRA must provide written policy, procedure, or other written documentation describing the requirement to and method used to audit public record researchers in order to actively monitor quality of researcher work.	CRA must present written documentation for auditing public record researchers. CRA shall make available the person responsible for such audits and auditor may ask to see (but not retain copy of) audit results for one or more public record researchers. CRA must provide evidence of adherence to procedures.	Audit procedures for public record researchers must include, but are not limited to: 1) an established protocol for auditing researchers, 2) volume of audit to be conducted, 3) sending research requests where result is already known, 4) how returned results are compared to expected results, and 5) process for dealing with researcher errors up to and including termination of services. Test cases must be entered in a log with results including: A) date of test, B) unique identifier such as order number or subject name plus last four digits of SSN, C) results returned, D) whether results were as expected, and E) any remedial actions taken. Auditor will seek evidence of adherence to policies and procedures.
Verification Services Standards			
5.1 Verification Accuracy			
CRA must have and follow reasonable procedures to assure maximum possible accuracy when obtaining, documenting and reporting verification information.	CRA must provide written policy, procedure, or other documentation used to reasonably ensure accuracy and thoroughness in the verification process.	CRA must make available to auditor tools or systems used (except actual personally identifiable information) to reasonably ensure verification accuracy. If interviewed, CRA workers responsible for verification accuracy must demonstrate knowledge of accuracy requirement; describe methodology by which they learn how to obtain accurate verifications. CRA workers responsible for verification accuracy shall be able to access current copy of documentation; AND/OR CRA workers must identify person/s responsible for accuracy. CRA must provide evidence of adherence to procedures, including training records.	CRA must provide information regarding verification accuracy to workers who are responsible for such accuracy by using various methods which may include, but are not limited to: 1) written manuals, 2) online manuals or instructions, 3) classroom training, 4) on-the-job training, and/or availability of expert to provide assistance when needed. If classroom or on-the-job training is used, a training outline or manual must be used. Methods used to reasonably ensure verification accuracy must include, but are not limited to: 1) confirmation of identity through verification of SSN, full name, and/or date of birth; and 2) confirmation of information source name, address, and contact information. Auditor will seek evidence of adherence to policies and procedures, which may include training records.
5.2 Current Employment			
CRA must have and follow procedures to contact consumer's current employer directly only when authorized by consumer or when client receives authorization from consumer and provides such authorization to CRA.	CRA must provide written policy, procedure, or other documentation used to ensure consumer's current employer is not contacted directly unless consumer has provided explicit authorization or when client receives authorization from consumer and provides such authorization to CRA.	CRA must make available to auditor tools or systems used (except actual personally identifiable information) to reasonably ensure current employer is not directly contacted without explicit authorization by the consumer or the client on behalf of the consumer. If interviewed, CRA workers responsible for verification of current employment must demonstrate knowledge of authorization requirement and describe	CRA must provide information regarding verification of current employment to CRA workers who are responsible for such verification by using various methods which must include, but are not limited to, at least one of the following: 1) written manuals, 2) online manuals or instructions, 3) classroom training, 4) on-the-job training, and/or availability of expert to provide assistance when needed. If classroom or on-the-job training is used, a training outline or manual may be used. Methods used to reasonably ensure consumer's current employer is directly contacted only with authorization may include, but are not limited to: 1) authorization provided on employment application, 2) explicit authorization provided within Disclosure/

NAPBS BACKGROUND SCREENING AGENCY ACCREDITATION PROGRAM (BSAAP) – ACCREDITATION STANDARD AND AUDIT CRITERIA

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)
		methodology by which they learn about such requirement. CRA workers responsible for current employer contact must be able to access current copy of documentation; and/or CRA workers must identify person/s responsible for such contact. CRA must provide evidence of adherence to procedures, including training records.	Authorization signed by consumer, 3) specific directive provided by client following receipt of authorization from consumer, and/or 4) technology must prevent verification of current employment by CRA workers until CRA Leader has so enabled. Auditor will seek evidence of adherence to policies and procedures, which may include training records.
5.3 Accredited Academic Institutions			
CRA must have and follow procedures to inform client when post-secondary academic institutions are not accredited by an accrediting body recognized by U.S. Department of Education, Council of Higher Education Accreditation (CHEA), similar U.S. body, or comparable global body, if reasonably available, for academic institutions outside the U.S.	CRA must provide written policy, procedure, or other documentation used to determine whether post-secondary academic institution is accredited by accrediting body recognized by U.S. Department of Education, CHEA, or similar body. CRA must provide written policy, procedure, or other documentation used to inform client when any post-secondary academic institution submitted for verification is not accredited by an accrediting body recognized by the US Department of Education, CHEA, similar U.S. body, or comparable global body, if reasonably available, for academic institutions outside the U.S.	CRA must provide policy or procedure used to reasonably ensure accreditation status of post-secondary academic institution and to inform client when any academic institution submitted for verification is not accredited by an accrediting body recognized by the U.S. Department of Education, CHEA, similar U.S. body, or comparable global body, if reasonably available, for academic institutions outside the U.S. If interviewed, CRA workers responsible for verification of academic credentials must demonstrate knowledge of accrediting bodies and describe methodology by which they learn how to confirm accreditation status of academic institutions. CRA workers responsible for verification of academic credentials must be able to access current copy of documentation; AND/OR CRA workers must identify person/s responsible for such activity. CRA must provide evidence of adherence to procedures, including training records.	CRA must provide information regarding verification of accreditation status of post-secondary academic institutions to CRA workers who are responsible for such verification by using various methods which include, but are not limited to, at least one of the following: 1) written manuals, 2) online manuals or instructions, 3) classroom training, 4) on-the-job training, and/or availability of expert to provide assistance when needed. If classroom or on-the-job training is used, a training outline or manual must be used. Methods used to reasonably ensure legitimacy of accrediting body include, but are not limited to confirmation using: 1) U.S. Department of Education, 2) the Council for Higher Education Accreditation, 3) state education departments, 4) similar U.S. body, and/or comparable global body, if reasonably available, for academic institutions outside the U.S. Auditor will seek evidence of adherence to policies and procedures, which may include training records.
5.4 Procedural Disclosures			
CRA must have and follow procedures to provide full disclosure to clients about general business practices regarding number of attempts to verify information, what constitutes an "attempt," locate fees, fees charged by the employer or service provider and standard question formats prior to providing such services.	CRA must present written policy, procedure, client education material or other written documentation used to provide full disclosure to a client about general business practices regarding number of attempts to verify information, what constitutes an "attempt," locate fees, fees charged by the employer or service provider and standard question formats prior to providing such services.	CRA must make available to auditor tools or systems used to disclose to client general practices regarding verification practices including attempts to verify, fees, question formats, etc. CRA must present written procedure for providing information to clients that accurately describes products, including one or more samples of provided documents. If consumer reports are used to demonstrate full and accurate procedural disclosure, all personally identified information must	CRA must provide information to clients regarding general verification business practices by using various methods which may include, but are not limited to: 1) product descriptions, 2) statement of work documents, 3) written agreements, and/or detail provided in the verification itself. Disclosed information regarding general verification business practices must include, but is not limited to: 1) number of attempts to verify information, 2) what constitutes an "attempt," 3) fees charged by the employer or service provider, and 4) standard question formats. Auditor will seek evidence of adherence to policies and procedures.

NAPBS BACKGROUND SCREENING AGENCY ACCREDITATION PROGRAM (BSAAP) – ACCREDITATION STANDARD AND AUDIT CRITERIA

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)
		be redacted and auditor will not retain copy. If interviewed, CRA workers must demonstrate knowledge that procedural requirements exist, where such requirements are documented, and/or the person responsible for CRA's products. CRA must provide evidence of adherence to procedures.	
5.5 Verification Databases			
If CRA compiles, maintains and resells employment or educational verification information, CRA must have and follow procedures to ensure that data compiled and stored is accurate, including procedures for handling consumer disputes.	CRA must present written policy, procedure or other written documentation used to ensure that data compiled and stored is accurate, including procedures for handling consumer disputes. If CRA does not compile, maintain, and resell employment or education information, CRA must provide written affirmation to that effect.	CRA must make available to auditor tools or systems used (except actual personally identifiable information) to reasonably ensure data compiled and stored is accurate. If interviewed, CRA workers responsible for accuracy of stored data must demonstrate knowledge of accuracy requirement and describe methodology used to ensure accuracy. CRA workers responsible for accuracy of stored data must be able to access current copy of documentation, identify person/s responsible for accuracy of stored data, AND/OR utilize technology to control the addition or deletion of information in the database/s. CRA must provide evidence of adherence to procedures, including training records.	This clause addresses organizations that compile information for potential future use or sale. CRA must provide information regarding accuracy of stored data to CRA workers who are responsible for such accuracy by using various methods which include, but are not limited to, at least one of the following: 1) written manuals, 2) online manuals or instructions, 3) classroom training, 4) on-the-job training, and/or availability of expert to provide assistance when needed. If classroom or on-the-job training is used, a training outline or manual must be used. Methods used to reasonably ensure accuracy of stored data include, but are not limited to: criteria for inclusion into the database, criteria for redaction from the database, criteria for correcting inaccuracies and handling consumer disputes. Auditor will seek evidence of adherence to policies and procedures, which may include training records.
5.6 Use of Stored Data			
If CRA provides investigative consumer reports from stored data, CRA must have and follow procedures to ensure the CRA does not provide previously reported adverse information unless it has been re-verified within the past three months, or for a shorter time if required by applicable law.	CRA must present written policy, procedure or other written documentation to ensure CRA does not provide previously reported adverse information stored in CRA's database unless it has been re-verified within the past three months, or for a shorter time if required by applicable law. If CRA does not utilize stored data, CRA must provide written affirmation to that effect.	CRA must make available to auditor tools or systems used (except actual personally identifiable information) to reasonably ensure that adverse data older than 3 months (or less if so required by applicable law) in CRA's database is re-verified prior to such information being included in a new consumer report. If interviewed, CRA workers responsible for use of such data shall demonstrate knowledge of 3-month re-verification requirement and describe methodology used to ensure compliance. CRA workers responsible for use of stored data must be able to access current copy of documentation; must identify person/s responsible for use of stored data, AND/OR technology must prevent utilization of stored adverse data which is older than 90 days. CRA must provide evidence of adherence to procedures, including	CRA must provide information regarding use of stored adverse data to CRA workers who are responsible for using such data by using various methods which include, but are not limited to, at least one of the following: 1) written manuals, 2) online manuals or instructions, 3) classroom training, 4) on-the-job training, and/or 5) availability of expert to provide assistance when needed. If classroom or on-the-job training is used, a training outline or manual must be used. Such information and/or training shall include what constitutes "adverse" information for different types of background checks through: 1) definition, 2) examples, and/or 3) by referring CRA workers to designated expert. Auditor will seek evidence of adherence to policies and procedures, which may include training records.

NAPBS BACKGROUND SCREENING AGENCY ACCREDITATION PROGRAM (BSAAP) – ACCREDITATION STANDARD AND AUDIT CRITERIA

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)
		training records.	
5.7 Documentation of Verification Attempts			
CRA must have and follow procedures to document all verification attempts made and the result of each attempt, in completing all verification services.	CRA must present written policy, procedure, or other written documentation used to ensure that all attempts made to verify information are fully documented.	CRA must make available to auditor tools, systems, or methods used to capture attempts to verify and related information. If a manual process, CRA must present written procedure for capturing such information. If consumer reports are used to demonstrate captured attempts and related information, all personally identified information shall be redacted and auditor will not retain copy. If interviewed, CRA workers must demonstrate knowledge that attempts to verify must be documented, where such requirements are documented, identify the person responsible for CRA's products and processes, AND/OR technology must automatically capture attempts to verify and related information. CRA must provide evidence of adherence to procedures, including training records.	CRA must provide information regarding attempts to verify and related information to CRA workers who are responsible for data verification by using various methods which include, but are not limited to, at least one of the following: 1) written manuals, 2) online manuals or instructions, 3) classroom training, 4) on-the-job training, and/or availability of expert to provide assistance when needed. If classroom or on-the-job training is used, a training outline or manual must be used. Information regarding attempts to verify must include, but is not limited to: 1) date and time of contact or attempted contact, 2) method of contact (such as phone number dialed, fax number used, email address used, address to which information was mailed, etc.), 3) name and title of contact, 4) results of attempt, and 4) the CRA employee who made the attempt or obtained information. Auditor will seek evidence of adherence to policies and procedures, which may include training records.
5.8 Outsourced Verification Services			
CRA must have and follow procedures requiring a signed agreement from all providers of outsourced verification services. The agreement must clearly outline the scope of services to be provided, verification methodology, documentation of verification efforts, disclosure of findings, time frame for communication and completion of requests, confidentiality requirements, reinvestigation requirements and other obligations as furnishers of information under the federal FCRA.	CRA must provide written policy, procedure, or other written documentation describing how a signed agreement covering scope of services is obtained from and retained for all current outsourced verification service providers. CRA must also provide copy of current agreement. If CRA does not outsource verification services, CRA must provide written affirmation to that effect.	CRA must present written procedure for obtaining signed agreement, copy of agreement, and demonstrate where/how signed agreements are retained. CRA must make available the person responsible for obtaining and retaining these agreements and auditor may ask to see (but not retain a copy of) signed agreements from one or more outsourced verification service providers. If interviewed, CRA workers responsible for working with these providers must demonstrate understanding of requirement for signed agreement prior to utilizing services of provider OR technology must prevent utilization of provider by CRA workers until CRA Leader has enabled use. CRA must provide evidence of adherence to procedures.	The agreement must include, but is not limited to: 1) the requirement to conduct all verifications in full compliance with applicable law and regulation, 2) scope of services provided, 3) methods used to obtain information, 4) time frame for communication and completion of requests, 5) methodology for confirming identity of subject of verification, 6) confidentiality requirements, 7) reinvestigation requirements, 8) documented "attempts to verify" per Clause 5.4, 9) background check requirements and acceptable results for provider's employees, and 10) signed non-disclosure agreements from provider's employees. In particular, the agreement must emphasize confidentiality requirements including: A) the legal requirement to treat all consumer information as confidential, B) secure data transmission, and C) secure and timely disposal of confidential information. Auditor will seek evidence of adherence to policies and procedures.
5.9 Conflicting Data			

NAPBS BACKGROUND SCREENING AGENCY ACCREDITATION PROGRAM (BSAAP) – ACCREDITATION STANDARD AND AUDIT CRITERIA

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)
Should CRA receive information from the verification source subsequent to the delivery of the consumer report, and as a direct result of the initial inquiry, that conflicts with originally reported information, and that new information is received within 120 days of the initial report, (or as may be required by law), CRA must have and follow procedures to notify client of such information.	CRA must provide written policy, procedure, or other documentation describing how conflicting data, when received within 120 days of report completion and as a direct result of original inquiry, is provided to client who originally ordered such report.	CRA workers responsible for reporting conflicting data must demonstrate knowledge of proper procedures and be able to access current copy of documentation. CRA must provide evidence of adherence to procedures, including training records.	CRA must provide information regarding processing and reporting of conflicting data to CRA workers who have this responsibility by using various methods which include, but are not limited to, at least one of the following: 1) written manuals, 2) online manuals or instructions, 3) classroom training, 4) on-the-job training, and/or availability of expert to provide assistance when needed. If classroom or on-the-job training is used, a training outline or manual must be used. Information regarding handling and reporting of conflicting data must include, but is not limited to: 1) confirmation that conflicting information is specifically related to same consumer, same customer, and original report, 2) verification of the authenticity of the conflicting information and its source, 3) method used to update report, and 4) method used to provide updated information to consumer and customer, and 5) the form in which the update is provided. Auditor will seek evidence of adherence to policies and procedures, which may include training records.
5.10 Authorized Recipient			
If CRA is requesting verification by phone, fax, email or mail, CRA must have and follow procedures to confirm that verification request is directed to an authorized recipient.	CRA must provide written policy, procedure, or other documentation used to require that verification requests are directed to authorized recipients.	CRA must present written procedure for confirming a verification request is being sent to an authorized individual. If interviewed, CRA workers responsible for processing verification requests must demonstrate knowledge of proper authentication procedures and must be able to access current copy of documentation. CRA must provide evidence of adherence to procedures, including training records.	Procedures used to ensure verification requests are sent to an authorized recipient must include, but are not limited to: 1) confirming method used by information source to provide verification information, 2) confirming company/institution name and address matches that provided by consumer, and 3) obtaining name and title of person to whom request will be sent. Auditor will seek evidence of adherence to policies and procedures, which may include training records.
Business Practices			
6.1 Background Checks for CRA Personnel Charged with Enforcement of Policy			
CRA must have and follow a policy requiring criminal background checks and government sponsored sanction list checks be conducted on all CRA owners, officers, principals and CRA workers charged with enforcement of company policy. Checks must be conducted at official, appropriate government repositories to cover 7 years of residential history and such records must be retained unless otherwise prohibited by applicable law. Record checks must be conducted at least once every two years covering the time period since the last check was completed and records retained for the duration of enforcement responsibility. Any criminal conviction(s) or sanctions listing(s) must be evaluated to determine if the individual may remain in an enforcement capacity based on: 1)	CRA must provide written policy, procedure, or other written documentation describing the requirement for and methodology used to conduct and retain criminal record and sanctions list checks on owners, principals, and CRA workers charged with enforcement of company policy. The documentation must describe how results of these checks are evaluated in relation to "Green Factors" and the individual's enforcement role. The documentation must include special processes used to evaluate convictions for any crimes involving dishonesty, fraud, moral turpitude, or listing on a government sponsored sanction list.	CRA must present written procedure for conducting criminal record and sanctions list checks at least once every two years on owners, principals and CRA workers charged with the enforcement of company policy. CRA must demonstrate how results are reviewed, including application of "Green Factors," and where records are retained. CRA must make available the person responsible for these checks and auditor may ask to see (but not retain a copy of) check results. CRA must provide evidence of adherence to procedures.	This clause refers only to the entity being accredited and not any parent company. It covers owners, managers, and CRA workers charged with enforcement of company policy. If conviction(s) or sanctions listing(s) are found, the evaluation of such information must comply with all applicable legal and regulatory requirements in relation to work performed by CRA and licenses held by the CRA (such as private investigator), as well as application of "Green Factors." Auditor will seek evidence of adherence to policies and procedures.

NAPBS BACKGROUND SCREENING AGENCY ACCREDITATION PROGRAM (BSAAP) – ACCREDITATION STANDARD AND AUDIT CRITERIA

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)
nature and gravity of offense or conduct, 2) time passed since offense, conduct, or completion of sentence and 3) nature of current enforcement role (commonly referred to as "Green Factors").			
6.2 Background Checks for CRA Workers			
CRA must have and follow a policy requiring criminal background checks and government sponsored sanction list checks be conducted on all CRA workers. Checks must be conducted at official, appropriate government repositories to cover 7 years of residential history and such records must be retained unless otherwise prohibited by applicable law. Such record checks must be conducted at least once every two years and records retained as long as CRA worker provides services to CRA. Any criminal conviction(s) or sanctions listing(s) must be evaluated to determine if the individual may remain his/her current position or any other position with CRA based on: 1) nature and gravity of offense or conduct, 2) time passed since offense, conduct, or completion of sentence and 3) nature of current or desired role (commonly referred to as "Green Factors").	CRA must provide written policy, procedure, or other written documentation describing the requirement for and methodology used to conduct and retain criminal record and sanctions list checks on CRA workers. The documentation must describe how results of these checks are evaluated in relation to "Green Factors" and the individual's role.	CRA must present written procedure for conducting criminal record and sanctions list checks at least once every two years on CRA workers. CRA must demonstrate how results are reviewed, including application of "Green Factors," and where records are retained. CRA must make available the person responsible for these checks and auditor may ask to see (but not retain a copy of) criminal history and sanctions list check results. CRA must provide evidence of adherence to procedures.	If conviction(s) or sanctions listing(s) are found, the evaluation of such information must comply with all applicable legal and regulatory requirements in relation to work performed by CRA and licenses held by the CRA (such as private investigator), as well as application of "Green Factors." Auditor will seek evidence of adherence to policies and procedures.
6.3 Changing Law and Regulation			
CRA must have and follow procedures to remain knowledgeable about and compliant with changing law and regulation. The CRA must designate an individual(s) or position(s) with the organization responsible for such knowledge and compliance or identify the external resource utilized for this purpose.	CRA must employ or retain a minimum of one person who is responsible for CRA's knowledge of and compliance with changing law and regulation as evidenced by written job description/s or other documentation. If multiple people are responsible, one person must hold CRA Leadership role and overall responsibility as evidenced by written job description or other documentation.	CRA must present written job description, policy, procedure or other documentation which identifies, by name and/or title, the person responsible for CRA's knowledge of and compliance with changing law and regulation or external resource retained for such purpose. CRA must make this person available either in person or by phone. If interviewed, CRA workers must identify the person/s that can provide expertise in regard to changing to changing law and regulation.	Responsible individual must affirm his/her role as being responsible for knowledge of changing law and regulation and compliance with same.
6.4 Insurance			
CRA shall maintain a minimum of $1 million coverage in errors and omissions insurance. If CRA does not maintain errors and omission insurance, CRA must self-insure in a manner compliant with its state's insurance requirements.	CRA must provide copy of Certificate of Insurance listing errors and omissions policy coverage amount. If CRA does not maintain errors and omissions insurance, CRA must provide documentation that they have self-insured in conformance with state requirements.	None	None
6.5 Client Authentication			

NAPBS BACKGROUND SCREENING AGENCY ACCREDITATION PROGRAM (BSAAP) – ACCREDITATION STANDARD AND AUDIT CRITERIA

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)
CRA must have and follow a procedure to identify and authenticate all clients prior to disclosing consumer reports or other consumer information. The procedure must require the CRA to maintain written records regarding the qualification of each client who receives consumer reports or other consumer information.	CRA must provide written policy, procedure, or other written documentation describing the requirement for and method used to authenticate clients prior to providing consumer reports or any consumer information to client.	CRA must present written procedure for authenticating new clients, and demonstrate where/how authentication results are retained. CRA must make available the person responsible for such authentication and auditor may ask to see (but not retain a copy of) authentication records from one or more client companies. If interviewed, CRA workers responsible for providing consumer information to clients must demonstrate understanding of authentication requirement prior to providing consumer information to clients or technology must prevent providing such information to clients until CRA Leader has enabled process. CRA must provide evidence of adherence to procedures.	Client authentication methods must include, but are not limited to: 1) obtaining evidence of right to conduct business, such as copy of business license, articles of incorporation, or state filing etc., and authentication thereof, 2) verification of working business phone, fax, email, and website, 3) verification of listing in business directories such as yellow pages, Hoover's, Dun and Bradstreet, etc., and may include 4) onsite inspection to confirm business facility exterior and interior appearance meet common business norms for this type of business. Auditor will seek evidence of adherence to policies and procedures.
6.6 Vendor Authentication			
CRA must have and follow a procedure to identify and authenticate all vendors prior to disclosing consumer information. The procedure must require the CRA to maintain written records regarding the qualification of each vendor who receives consumer information.	CRA must provide written policy, procedure, or other written documentation describing the requirement for and method used to authenticate vendors prior to disclosing any consumer information to vendor.	CRA must present written procedure for authenticating new vendors, and demonstrate where/how authentication results are retained. CRA must make available the person responsible for such authentication and, if interviewed, this person must demonstrate understanding of authentication requirements. Auditor may ask to see (but not retain a copy of) authentication records from one or more vendor companies. CRA must provide evidence of adherence to procedures.	In the case of vendors that are recognized and commonly utilized by CRAs, a signed agreement between the vendor and CRA will suffice as authentication. Such vendors include: major credit bureaus, repositories of education and employment data, and motor vehicle record resellers. For unknown vendors, authentication records must include, but are not limited to, the following: 1) evidence of right to conduct business, such as copy of business license, articles of incorporation, or state filing etc., and authentication thereof, 2) verification of working phone/fax numbers, website, email, 3) reference through a minimum of one independent third-party, and 5) previous experience of CRA when working with vendor. Authentication records may also include onsite inspection results. Auditor will seek evidence of adherence to policies and procedures.
6.7 Consumer Authentication			
CRA must have and follow reasonable procedures to obtain proof of identity prior to providing any information to a consumer making a telephonic inquiry. The CRA must maintain reasonable procedures to document the information used to identify each consumer to whom consumer information is provided.	CRA must provide written policy, procedure, or other written documentation describing how/when consumer authentication/ identification occurs prior to disclosing consumer information and where record of such authentication is kept.	CRA must present written procedure for confirming consumer identity prior to providing any consumer information to such person. Auditor may ask to see demonstration of consumer identification, how CRA representative confirms identity of consumer, and where record of authentication is retained. CRA must provide evidence of adherence to procedures.	Consumer identification processes must include, but are not limited to, confirmation of full name as provided on consumer report and at least two of the following: 1) date of birth, 2) street address used on application or authorization document, 3) last four digits of SSN/Country ID, 4) driver's license number, and 5) report ID number. Auditor will seek evidence of adherence to policies and procedures OR through use of properly issued client provided log in credentials.
6.8 Document Management			
CRA must have and follow a written record retention and	CRA must provide written policy, procedure, or other	CRA must present written document retention and	Processes must address both electronic and hard copy records and include: 1) period of

NAPBS BACKGROUND SCREENING AGENCY ACCREDITATION PROGRAM (BSAAP) – ACCREDITATION STANDARD AND AUDIT CRITERIA

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)
destruction policy which, at a minimum, complies with all applicable law and regulation.	written documentation describing CRA's record retention and destruction practices.	destruction policy. CRA must make available the person responsible for document retention and destruction. If interviewed, this person must demonstrate understanding of retention and destruction requirements and processes. CRA must provide evidence of adherence to procedures.	retention for consumer records, 2) method used to determine record age, 3) processes used for actual record destruction, 4) documentation of record destruction activity, and 5) individual responsible for initiating, managing, confirming, and documenting record destruction, CRA's are subject to the FTC's document destruction rule which currently requires secure destruction through means that are reasonable and appropriate to prevent the unauthorized access to or use of information in a consumer report. (The FTC rule is found at 16 CFR Part 682.) Auditor will seek evidence of adherence to policies and procedures.
6.9 Employee Certification			
CRA must have and follow a policy requiring all CRA workers to certify in writing they will adhere to the confidentiality, security and legal compliance practices of the CRA.	CRA must provide written policy, procedure, or other written documentation describing how/when CRA obtains from all CRA workers certification(s) in which worker agrees to adhere to the CRA's confidentiality, security, and legal compliance practices and where such certifications are retained. CRA must provide copy of certification document(s).	CRA must present written procedure for obtaining CRA worker written certification(s) that worker will adhere to CRA's confidentiality, security, and legal compliance practices. If questioned, CRA workers must confirm they were required to provide this certification(s). Auditor may ask to see, but not retain copy of, certification(s) signed by one or more workers. CRA must provide evidence of adherence to procedures.	Certification(s) language must include, but is not limited to, agreement by CRA workers to: 1) hold, use, and destroy all client and consumer information in a secure manner, 2) provide consumer information to third parties only after following defined authentication procedures, 3) abide by physical security practices, 4) abide by information security practices, and 5) follow all compliance practices of the CRA. Auditor will seek evidence of adherence to policies and procedures.
6.10 Professionalism and Proficiency Training			
CRA must have and follow procedures to provide initial and ongoing training to CRA workers, where training is commensurate with specific worker role and responsibilities. CRA must retain records of such training.	CRA must provide written policy, procedure, or other documentation to provide initial and ongoing training to CRA workers, where training is commensurate with specific worker role and responsibilities and retain records of such training.	CRA must make available to auditor any materials used to train CRA workers on specific job responsibilities and records of such training. If interviewed, CRA workers must describe training which was received. CRA must provide evidence of adherence to procedures.	CRA must provide information and training to workers which are specific based on worker role and responsibilities. CRA must provide training on general requirements of confidentiality, professionalism, accuracy, and worker's role as a representative of the CRA organization. CRA must retain records of all such training. Training methods may include, but are not limited to: 1) written material, 2) online training, 3) training classes/webinars, 4) one-on-one training sessions, and/or 5) on-the-job training. Auditor will seek evidence of adherence to policies and procedures.
6.11 Worker Confidentiality, Legal, and Compliance Training			
CRA must have and follow procedures to provide initial and annual training to all workers on confidentiality, security and legal compliance practices of the CRA and maintain records of such training.	CRA must provide written policy, procedure, or other documentation which describes the requirement for and methodology used to train CRA workers on the confidentiality, security, and legal compliance procedures of the CRA and how such records are retained.	CRA must present written procedure for providing initial and annual training to CRA workers regarding confidentiality, security and legal compliance practices of CRA and how such records are retained. CRA must make available to auditor any materials used for such training. If interviewed, CRA workers must describe training which was received. CRA must provide evidence of adherence to procedures.	CRA must provide initial and annual training to CRA workers regarding confidentiality, security, and legal compliance practices by using one or more methods which include, but are not limited to: 1) written material, 2) online training, 3) training classes/webinars, 4) one-on-one training sessions, and/or 5) on-the-job training. CRA must retain records of such training. Auditor will seek evidence of adherence to policies and procedures.

NAPBS BACKGROUND SCREENING AGENCY ACCREDITATION PROGRAM (BSAAP) – ACCREDITATION STANDARD AND AUDIT CRITERIA

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)
6.12 Visitor Security			
CRA must have and follow procedures for a visitor security program to ensure visitors do not view or have access to consumer information.	CRA must provide written policy, procedure, or other documentation which describes the visitor security program and how visitors are prevented from viewing or accessing consumer information.	CRA must present written procedure for ensuring visitor security which prevents viewing or accessing of consumer information. CRA must make available the person responsible for visitor security program. This person must be able to describe and/or provide documentation related to visitor security and access control. If questioned, CRA workers must demonstrate knowledge of visitor security policy. CRA must provide evidence of adherence to procedures.	Visitor security policy must include method/s which prevents visitors from viewing or accessing consumer information. These methods may include, but are not limited to: 1) use of sign in/out registry, 2) issuance of temporary badges, 3) situations in which a CRA employee must escort the visitor, 4) controlled access to systems and data, and 5) controlled access to areas of facility in which consumer information is readily available on screens or hard copy. Auditor will seek evidence of adherence to policies and procedures.
6.13 Responsible Party			
CRA must employ one person designated to oversee and administer the accreditation process and ongoing compliance by the CRA, including enforcement of the Accreditation Standard. This person must be vested with the responsibilities and authority attendant to this task, and must be the CRA contact for the auditor and accreditation related matters for NAPBS.	CRA must employ a minimum of one person who is responsible for CRA's accreditation activity and on-going compliance with applicable standards/requirements as evidenced by written job description/s or other documentation. If multiple people are responsible, one person must hold overall responsibility as evidenced by written job description or other documentation.	CRA must present written job description, policy, procedure or other documentation which identifies, by name and/or title, the person responsible for accreditation activity and on-going compliance. CRA must make this person available either in person or by phone. If interviewed, CRA workers must identify the person/s that can provide accreditation expertise when needed.	The person responsible for overall accreditation must affirm his/her role as being responsible for accreditation/certification activity and on-going compliance within the organization and that s/he is qualified to hold such responsibility.
6.14 Document Control			
CRA must have and follow procedures for document control and versioning to ensure correct versions of all controlled documents are used.	CRA must provide written policy, procedure, or other documentation describing the methods used to control documents and ensuring correct version of all controlled documents is used.	CRA must present procedures to ensure only the most recent version of any controlled document is used internally and made available externally. CRA must make available the person/s responsible for document control. If interviewed, CRA workers must demonstrate knowledge of document control requirements, describe methods used to ensure document control, must be able to access current copy of documentation, and must identify person/s responsible for document control systems. CRA must provide evidence of adherence to procedures, including training records.	CRA must provide training to CRA workers regarding how to identify, retrieve and use only most current version of any controlled document using one or more methods which include, but are not limited to: 1) user manual/guide, 2) online training, user guides, or help system, 3) user training classes/webinars, 4) one-on-one training sessions, or 5) verbal assistance. Auditor will seek evidence of adherence to policies and procedures, including training records.
6.15 Ethics Reporting			
CRA must have a process by which CRA workers can anonymously, to the extent possible, report ethical, compliance, and work product concerns without fear of identification or retaliation based on such reporting. CRA must have and follow	CRA must provide written policy, procedure, or other documentation describing how/when CRA informs CRA workers of reporting process, how CRA investigates reported concerns, and how CRA worker anonymity is	CRA must present written procedure for informing CRA workers of reporting process, availability, investigating reported concerns, protecting anonymity, and prohibiting retaliation based on such reporting. If	CRA must provide information to CRA workers regarding availability and use of CRA ethics reporting process. Methods to provide information must include at least one of the following: 1) inclusion in CRA Worker Handbook, 2) posting in CRA worker common area such as breakroom, 3) online training or help system, 4) one-on-one information sharing. Auditor will

NAPBS BACKGROUND SCREENING AGENCY ACCREDITATION PROGRAM (BSAAP) – ACCREDITATION STANDARD AND AUDIT CRITERIA

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)
a procedure to inform CRA workers of reporting process and anonymity; CRA must have and follow procedures for investigation of reported concerns.	maintained.	interviewed, CRA workers must demonstrate knowledge of reporting process and be able to access current copy of documentation. CRA must provide evidence of adherence to procedures.	seek evidence of adherence to policies and procedures.

GLOSSARY

For purposes of this Standard, the terms and acronyms below have the following definitions.

Note that where clause requirements include "signature" or "signed by" wet or electronic signature shall be deemed to meet signature requirement.

1. **Automated Reporting**: This refers to an inquiry being made, results being returned, and results being placed in a consumer report without any manual intervention or review by a person.
2. **CFPB**: The federal Consumer Financial Protection Bureau.
3. **Consumer Information**: Any information about an individual consumer provided to the CRA by the consumer, client, or other parties in the course of compiling a consumer report.
4. **Consumer Report**: The meaning given to it in § 603(d) of the federal FCRA.
5. **CRA:** A consumer reporting agency as defined in § 603(f) of the federal FCRA.
6. **CRA Worker/Worker**: Any individual who performs services for CRA and who has access to CRA premises and/or systems. These terms encompass employees as well as temporary workers, interns, contractors and others who perform work for the CRA.
7. **Depth of Search**: This refers to the number of years covered by a search. Examples include a 7-year search and 10-year search where record search must cover at least 7 years or 10 years respectively.
8. **FCRA**: The federal Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq.
9. **FTC**: The Federal Trade Commission.
10. **Investigative Consumer Report:** The meaning given to it in § 603(e) of the federal FCRA.
11. **Outsourced Verification Services**: Refers to a business arrangement in which the CRA contracts with another company and that company conducts employment, academic, and/or reference checks on behalf of the CRA and return results to the CRA (see Clause 5.8). Outsourcing criminal record checks to public record field researchers **ARE NOT** considered "Outsourced Verification Services."
12. **Policy**: A written directive that is required to be followed by the entity.
13. **Procedure:** A written description of how a policy is implemented and followed by the entity. (Procedures may be referred to within the entity as standard operating procedures, SOPs, operating guidelines or other names.)
14. **Public Record Researcher**: Any person or entity contracted or employed by a CRA, other than another CRA providing consumer reports in pursuant to FCRA Sec. 607(e), who searches for and/or retrieves information that is currently in the custody of a government entity such as a court, state agency or other government repository.
15. **Search Methodology**: Refers to the manner by which the search is conducted. Examples include: hands-on, in-person search (such as when a public access terminal is used at a courthouse), electronic access to original source (such as a remote electronic search of court records), electronic access to commercial database (such as The Work Number, Student Clearinghouse, and non-governmental criminal record database), electronic access to a government database (such as OFAC sanctions or PACER), telephonic inquiry to a source (such as school, employer, or reference) and email inquiry to a source (such as school, employer, or reference).
16. **Verification**: Academic, employment, reference, and other checks conducted using source information which is not public.