EXHIBIT (B)

Company Name:_____

	Initial	Criteria	Audit Methodology
		EMPLOYEE REQUIREMENTS	
1.1	Applicant Claims _____ _____ NAID USE ONLY Verified _____	***All Access Employees and Non-Access Employees*** must have the following on file: • **Confidentiality Agreement** • **I-9 Form** U.S. employees hired after November 7, 1986 or proper work registration for non-citizens *(See Employment Information Disclaimer.)*	The Auditor will request evidence of the appropriate documentation in the employee files as follows: • 7 or fewer Access and/or Non-Access Employees: Auditor will view employee files for all Access and Non-Access Employees. OR • More than 7 Access and/or Non-Access Employees: Auditor will view employee files as a random sample , totaling 25% of the entire Access and Non-Access Employees List, with a minimum of 7 employees and a maximum of 15 employees.
1.2	Applicant Claims _____ _____ NAID USE ONLY Verified _____	***Access Employees*** must have the below employment screening requirements: • **7 Year Criminal Record Search:** o Social Security Header Search listing all associated addresses of the employee. (Must be conducted prior to the criminal background investigation to ensure all counties, states, and federal district courts of residence and employment have been included and verified in the investigation) o County records search for all counties on Social Security Header Search o Statewide records search for all states on Social Security Header Search o Federal Records Search for all Federal Districts in all states on Social Security Header Search • **Pre-hire or Initial Drug Screening** • **7 Year Employment History Verification** which must include the following for each place of employment: o Name, City and State of the previous employer o Dates of employment, as reported by the employee o Date of verification (or attempted verification if the previous employer cannot be reached) o Indication of if the previous employer was able to verify the dates employment. The criminal record search must be conducted by a third-party. County and state checks must be pulled directly from the county and state repositories. Federal checks must be pulled from the federal district courts or via PACER. The use of a secondary database, often referred to as a SuperSearch, InstaSearch and/or National/Nationwide Search is not allowed. If federal, statewide and/or county searches are not available in a particular state, the applicant must complete the ones available and provide documentation to support the unavailability of the other. Canadian searches must be done on a province/territory and National basis and obtained through a third-party background search service or Canadian Police Information Centre (CPIC). When searches are being conducted in places outside of the U.S. every effort should be made to have the searches done at a level comparable to the county and state searches done in the U.S. If a location has restrictive employee agreements in place that prevents drug screening and/or criminal record searches for certain employees, a letter must be submitted stating who and what employee screening restrictions are in place.	Auditor must inspect applicable documentation for all Non-Citizen Employees and Access Employees who are owners, partners or senior managers (of destruction division) of the Company. The following Access Employees are exempt from the Employment Verification, Drug Screening and I-9: 1) officers, directors, owners and/or partners of the Company not engaged in the day-to-day operations; 2) others who have access to or can grant authorize access to the Confidential Customer Media to be destroyed at the applicant's location but are not engaged in the day-to-day destruction operations; and/or 3) independent contractors, subcontractors or employees. Any Access Employees representing the Headquarters of the Company's information destruction division, minimally the President/Vice President of area &/or Audit Coordinator, whether at the location listed on this application or at another location, must have criminal background searches conducted. Auditor will review the results of the Social Security Header Search and criminal background checks of the selected employees. Criminal background checks must include a list and the results of the jurisdictions searched. No person subject to a felony conviction in the last 7 years for any crime involving theft (of tangible or intangible property), fraud, burglary or larceny, and no person currently incarcerated for any crime may be employed in a capacity where they may come in contact with Confidential Customer Media. This applies to all Access Employees. The employment screening is applicable to all Access Employees (other than those exempt from these requirements as mentioned above) regardless of length of service or pre-existing employment status, except where there is a restrictive employment agreement in place. Access Employees whose employment predates the implementation of NAID Certification, must state that they have been employed with the company for the past 7 years.

Company Name:_____

	Initial	Criteria	Audit Methodology
1.3	Applicant Claims _____ NAID USE ONLY Verified _____	Access Employees are monitored for drugs/substance abuse by one of the following methods (check one): ☐ Option #1: On a random basis, 50% of access employees are drug screened annually. **OR** ☐ Option #2: Management has been trained in a "Substance Abuse Recognition Awareness Program" pre-approved by NAID.	Auditor will verify evidence of the method indicated: Option #1: Invoices/results from drug testing lab for random sampling drug screening of 50% of employees **OR** Option #2: Documentation showing Program approval from NAID and proof that on-site management has completed this Substance Abuse Recognition training within the last year.
1.4	Applicant Claims _____ NAID USE ONLY Verified _____	Ongoing criminal record searches on Access Employees by one of the following methods (check one): ☐ Option #1: One-third of Access Employees have been randomly selected and criminal record searches conducted annually. ☐ Option #2: One-third of all Access Employees are screened the first year, a different 1/3 are screened the following year, and the remaining 1/3 are screened in the third year. ☐ Option #3: All Access Employees have criminal record searches conducted every three years. Year of most recent search: _____	Auditor will review the results of the criminal record search of the employees based upon the method indicated.
1.5	Applicant Claims _____ NAID USE ONLY Verified _____	Drivers meet all licensing requirements of the governmental jurisdiction.	The applicable law or regulation for commercial driver licenses will be made available and examined by the Auditor. Auditor will request any items required by law for all drivers listed on the Access and Non-Access Employees List.
		OPERATIONAL SECURITY	
2.1a	Applicant Claims _____ NAID USE ONLY Verified _____	The Company has a written policies and procedures for drivers and destruction processing employees.	Auditor to inspect a copy of policies and procedures manuals.
2.1b	Applicant Claims _____ NAID USE ONLY Verified _____	Prior to gaining access to confidential material, all drivers and destruction processing employees must sign an acknowledgement indicating that they have received, read and understand the Company's current written policies and procedures. A new acknowledgment must be signed by employees on an annual basis.	Auditor to inspect employee files for a signed acknowledgement of the Company's current written policies and procedures. This form must reference the version of the written policies and procedures that it applies to. A new acknowledgment must be signed by employees on an annual basis.

Company Name:_____

	Initial	Criteria	Audit Methodology
2.1c	Applicant Claims _____ NAID USE ONLY Verified _____	The Company has a written policy in place, stating that the Company will notify any Customer of a potential release of, or unauthorized access to, that Customer's Confidential Customer Media that poses a threat to the security or confidentiality of that information within 60 days of the date of discovery of the data security breach incident.	Auditor will check procedures manual to ensure there is a written policy stating the Company will notify any Customer of a potential release of, or unauthorized access to, that Customer's Confidential Customer Media that poses a threat to the security or confidentiality of that information within 60 days of the date of discovery of the data security breach incident.
2.1d	Applicant Claims _____ NAID USE ONLY Verified _____	The Company has a written policy in place instructing and requiring employees to notify management of a potential release of, or unauthorized access to, Confidential Customer Media that poses a threat to the security or confidentiality of the information.	Auditor will check procedures manual to ensure that there is a written policy instructing and requiring employees to notify management of a potential release of, or unauthorized access to, Confidential Customer Media that poses a threat to the security or confidentiality of the information.
2.1e	Applicant Claims _____ NAID USE ONLY Verified _____	The Company has a written Incident Response Plan for responding to suspected or known security incidents. The Incident Response Plan must include a post-incident business impact analysis and a process for documenting all incidents and their outcomes.	Auditor will review the Company's written Incident Response Plan to ensure there is a policy addressing post-incident business impact analysis and documentation of all incidents and their outcomes.
2.1f	Applicant Claims _____ NAID USE ONLY Verified _____	The Company has a written policy that addresses the procedures for employees to follow during an unannounced audit. This policy must name at least one person or position of contact with physical access to the information the auditor may ask to review, which is to be contacted in the event of an unannounced audit at the destruction plant or the office. Should circumstances prevent the designated point of contact from being available at the time of the unannounced audit, the Certification Review Board may request additional information to be provided at a later date.	Auditor will review the Company's written policies and procedures for their written policy instructing employees in the procedures to follow during an unannounced audit.
2.1g	Applicant Claims _____ NAID USE ONLY Verified by _____	All Access Employees must be trained annually to comply with the NAID AAA Certification requirements: ☐ Option #1: All Access Employees have taken and passed the NAID Access Employee Training Program (AETP). (Submit AETP Licensing Form with application.) ☐ Option #2: All Access Employees have taken and passed a third-party training course which has been pre-approved by NAID. (Submit AETP approval form and outline of training with application.) ☐ Option #3: All Access Employees have taken and passed an in-house training. If NAID has not already approved the training course for this purpose, an approval form and outline of the program is included with this application. (Submit AETP approval form and outline of training with application.)	Auditor will review evidence of annual training to ensure all Access Employees have passed a training program which complies with the NAID AAA Certification requirements.

Company Name:_____

	Initial	Criteria	Audit Methodology
2.2	Applicant Claims _____ NAID USE ONLY Verified _____	Access Employees must display a Company-issued photo I.D. badge at all times while on duty. Badges must minimally include a photo, employee name and Company name.	Auditor will inspect the Company policies and procedures manual to ensure there is a written policy for Access Employees to display a Company-issued photo I.D. badge at all times while on duty. Auditor will also inspect employees present to verify that they are wearing photo I.D. badges.
2.3	Applicant Claims _____ NAID USE ONLY Verified _____	While at the Customer's location, drivers and other employees of contractor must wear a specific uniform (minimum of Company shirt) to improve recognition by Customers.	Auditor will inspect the Company policies and procedures manual to ensure there is a written policy for drivers and other employees of contractor must wear a specific uniform while at the Customer's location. Auditor will also inspect drivers present to verify they are wearing uniforms.
2.4	Applicant Claims _____ NAID USE ONLY Verified _____	At the time that media is transferred from the Customer's custody to the custody of the destruction Company's employees, the Customer must be provided with a receipt or certificate of destruction indicating type and quantity of media and an acknowledgement of the services rendered. An electronic receipt is acceptable, provided there is a verifiable electronic audit trail and the ability to provide the Customer with the printed information. If destruction services rendered by the Company are not NAID Certified, but such services could be NAID Certified and/or are recycling services of unshredded/intact paper, then the recipient of the services must be notified in writing that such service is NOT NAID Certified. This written notification may be contained on a materials receipt, certificate of destruction, current Customer agreement/contract or another written notice (including e-mail or another electronic method that may be printed) delivered by the Company to the Customer/recipient of services.	Auditor will inspect the Company policies and procedures manual to ensure that Customer documentation process contains the requisite information and will inspect a copy or sample of the Customer documentation. If applicable, Auditor must inspect a copy or sample of the Customer documentation when destruction or recycling services are NOT NAID Certified to verify such notification is stated. For Plant-based operations and Transfer Processing Stations only: If a Subcontractor is used for transport prior to destruction, the Subcontractor must provide the Customer and the Applicant Company with the Customer receipt documentation. Auditor to verify documentation has been provided by the Subcontractor and is being utilized by inspecting a copy of a past Customer receipt.
2.5	Applicant Claims _____ NAID USE ONLY Verified _____	All media for destruction must always be attended by an access employee or physically secured from unauthorized access while in the custody of the destruction contractor before they are destroyed.	The Auditor will verify that containers used in the field to transport media for destruction from the Customer's facility to the destruction provider's vehicle have operable locks. Auditor will inspect the Company policies and procedures manual to assure that custody of the media for destruction is addressed. For Plant-based operations and Transfer Processing Stations: Auditor will determine that there is a secured area designated for holding media when unattended until that media can be destroyed.
2.6	Applicant Claims _____ NAID USE ONLY Verified _____	All media is securely contained during transfer from Customers' custody to transportation vehicle to prevent loss from wind or other atmospheric conditions.	Auditor to inspect collection equipment used in the field to verify it protects the media from loss due to wind, tipping/spillage or other atmospheric conditions. If in the field, Auditor to check area around collection or destruction vehicle to verify it is free from loose information-bearing media.

Company Name:_____

	Initial	Criteria	Audit Methodology
2.7	Applicant Claims _____ NAID USE ONLY Verified _____	All vehicles used for transfer of media will have the applicable government inspection for roadworthiness on file.	Auditor will review paperwork from the most recent inspection of all the Company's commercial vehicles within the time frame stated in the applicable state law regarding the nature and frequency of these inspections. If there is a jurisdiction that does not require an inspection of commercial vehicles, Auditor will require a copy of the government statement saying so. Three vehicle records will be checked.
2.8	Applicant Claims _____ NAID USE ONLY Verified _____	All vehicles used for transfer and/or destruction of media (whether intact or destroyed) will have lockable cabs and lockable, fully enclosed boxes. These vehicle cabs and boxes must be locked during transport and when unattended by Access Employee.	Auditor will inspect trucks to verify that all cab doors and truck boxes are lockable and that locks work properly. Auditor will inspect the Company policies and procedures manual to assure that vehicle cab and box locking is addressed. Note: If there are 3 trucks or less in either category (Mobile Shredding and Collection Only), all trucks in each category must be made available for inspection. If there are 4 or more trucks in either category, 75% of the vehicles in either category must be made available for inspection. If trucks are not made available, the Company must provide written testimony that those trucks not presented for inspection are of equal or superior condition of roadworthiness and security. The testimony must be on Company letterhead and signed by an officer of the Company.
2.9	Applicant Claims _____ NAID USE ONLY Verified _____	All drivers of vehicles must have readily accessible two-way communication device.	Auditor to verify each driver has an operable two-way communication device with them or in the vehicle.
2.10	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified _____	***APPLIES TO MOBILE CERTIFICATION ONLY*** The Company must perform mobile destruction services at the Customer's site.	Auditor will verify that the Company policies and procedures manual indicates that mobile destruction services must be performed at the Customer's site, unless there is a written Customer agreement stating otherwise. A Records Center is considered the Customer's site when all media for destruction comes from within it.
2.11	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified _____	***APPLIES TO PLANT-BASED AND/OR TRANSFER PROCESSING STATION CERTIFICATION ONLY*** Unauthorized access to Confidential Customer Media in the designated secure destruction area, storage area and/or staging area is effectively prevented.	Auditor to inspect all entrances to verify that unauthorized access to secured area is effectively prevented when media is not attended. Auditor will verify that the Company policies and procedures manual covers access control and unauthorized access interdiction measures.

Company Name:_____

	Initial	Criteria	Audit Methodology
2.12	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified _____	***APPLIES TO PLANT-BASED AND/OR TRANSFER PROCESSING STATION CERTIFICATION ONLY*** All visitors entering the secure destruction building or Transfer Processing Station must sign a log with their name, time in, affiliation, and time out. Visitors must be issued a Visitor Badge and be escorted or under the supervision of an Access Employee at all times while in the building. The log must be maintained for one year.	Auditor will examine visitor logs and verify the logs are maintained for one year.
2.13	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified _____	***APPLIES TO PLANT-BASED AND/OR TRANSFER PROCESSING STATION CERTIFICATION ONLY*** There is a secure area within the building devoted only to processing and/or destroying media. No baling of unshredded paper may take place in secure areas of the plant-based destruction facility except cardboard. In the event that the facility also stores records, recycles, bales intact/unshredded paper or conducts other activities, the collection and processing of media for destruction must be in a designated (or delineated) area or secured area.	Auditor to inspect building to determine that the secured area for destruction and/or media processing exists and that no baling of unshredded paper takes place in the plant-based destruction area. If a secured area within the building is required, it must meet the following specifications: • There must be enough space within this area to stage all media to be destroyed. • The wall or fence securing this area must be a minimum of six feet tall and have a lockable gate or door. • If the wall or fence does not go all the way to the ceiling, then it must have a ceiling mounted sensor alarm inside and over the perimeter of the secure destruction, secure staging and processing areas (or similar, suitable device) to detect if and when individuals have climbed over or come through a section of the secured area fence/wall. If the only operations taking place within the building are related to information destruction, and if ALL employees with access into the building are screened in accordance with Section 1.2 and are listed as access employees, a separate secure area is not required and the entire building is considered the secure area.
2.14	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified _____	***APPLIES TO PLANT-BASED AND/OR TRANSFER PROCESSING STATION CERTIFICATION ONLY*** There is a third-party monitored alarm system in place and utilized when the secure destruction building or Transfer Processing Station is unoccupied.	Auditor is to inspect alarm system to make sure it is operational and examine alarm test reports &/or invoices from alarm monitoring service.
2.15	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified _____	***APPLIES TO PLANT-BASED AND/OR TRANSFER PROCESSING STATION CERTIFICATION ONLY*** There is a closed circuit camera system monitoring all access points into the secure buildings/areas where confidential media is stored, processed and/or destroyed. All processing activities are monitored with sufficient clarity to identify people and their activities. There must be enough lighting during non-business hours to ensure that all images have sufficient clarity. NAID must be notified within 48 hours of the discovery of problems with the CCTV system which result in a loss of data. Recordings must be retained for 90 consecutive days in an organized, retrievable manner. Number of days of recordings (as of the date of application):_____	Auditor to inspect the closed circuit monitoring system to ensure that it meets criteria. This includes checking that the system has sufficient cameras and image quality to identify individuals and capture all activities in the secure destruction building from point of entry through final destruction, including any unauthorized access to the confidential information. Auditor will also inspect the policies and procedures manual to ensure there is a written policy for notifying NAID within 48 hours of the discovery of problems with the CCTV system which result in a loss of data. 90 days of CCTV playback must be available at the time of the scheduled audit. Auditor to inspect recording library system and to review four 4-minute samples: • Two random samples during operational hours • One random sample during non-operational hours • One sample from the 90th day back from the current date Recording of operations may be suspended for playback recordings.

Company Name:_____

	Initial	Criteria	Audit Methodology
2.16	Applicant Claims _____ ☐Not Applicable NAID USE ONLY Verified _____	***APPLIES TO PLANT-BASED CERTIFICATION WITH A COLLECTION FACILITY*** Collection Facilities are used to store media intermittently to be transferred to a plant-based destruction facility within 3 business days. Facility has restricted access with a monitored alarm system. The list of all Collection Facility locations associated with this plant-based operation is included with this Application. Number of Collection Facilities:_____ **ADDRESS:** _____ _____	Auditor will check policy and procedures manual to assure that media for destruction is not processed and not stored for more that 3 business days and that the following are maintained: • Access is restricted to Access Employees • Visitor's Log • I.D. badges are worn by employees and visitors • Monitored Alarm System • In the event that the facility also stores records, recycles or bales intact/unshredded paper, or conducts other activities, the collection of media for destruction must be in a designated (or delineated) area or secured area. (See Item 2.13) Auditor may or may not check the actual facility for requirements at the time of an audit.
2.17	Applicant Claims _____ ☐Not Applicable NAID USE ONLY Verified _____	***APPLIES TO PLANT-BASED AND/OR TRANSFER PROCESSING STATION CERTIFICATION ONLY*** The following Operational Security systems are checked and maintained on a monthly basis: • Alarm System • Lighting • Door Locks • Visitor Logs The CCTV system must be checked on a weekly basis, including a minimum of five minutes of playback to ensure that all cameras and recording systems are working correctly. Monthly and Weekly Logs must be kept for one year.	Auditor will exam the Monthly and Weekly Operational Security Maintenance Logs and verify the are maintained for one year.
ENDORSEMENTS & THE DESTRUCTION PROCESS			
3.1	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified _____	***PAPER/PRINTED MEDIA ENDORSEMENT*** Paper/Printed Media is destroyed by commercial grade destruction equipment and meets the particle size as stated by the equipment's OEM specifications. Acceptable deviant tolerance: 1/16 inch ☐ **Continuous Shred:** Width (max): 5/8 inch & Length: Indefinite ☐ **Cross Cut or Pierce & Tear:** Width (max): 3/4 inch & Length (max): 2.5 inches ☐ **Pulverizer, Disintegrator or Hammermill*** Screen Size (max): 2-inch diameter holes ☐ **Unspecified Equipment** Please describe the type of equipment and cutting mechanism specifications (screen hole size*, blade width, etc.): _____ Maximum allowable sizes listed create a particle deemed reasonable for regulatory compliance. Customers may specify a smaller particle size at their discretion, which should be codified contractually with the NAID Certified service provider. Mobile or Plant Equipment:_____ Manufacturer: _____ Model: _____ Serial #: _____ Capacity/Throughput (lbs/hr): _____ Horsepower: _____ ☐ See attached form listing additional equipment info	The Auditor will verify that the particles produced by the equipment are reasonably consistent with the OEM specifications and that the equipment is of commercial grade. *Auditor will review the Screen Changing Logs during the audit, if applicable. **PULPING OR INCINERATION (PLANT-BASED ONLY)** In-House Pulping or Incineration must not require any Transfer of Custody: If the NAID Member owns or leases the pulping or incineration equipment and building, and does not transfer custody of media to a third party for transport or processing before media is pulped or incinerated, then the results of the pulping or incineration must effectively reduce the media to a size or condition that is not reconstructible.

Company Name:_____

	Initial	Criteria	Audit Methodology
3.2	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified _____	***MICRO MEDIA ENDORSEMENT*** Micro Media (Microfiche or Microfilm only) is destroyed by commercial grade destruction equipment which produces a particle size of 1/8 inch maximum dimension or less. Mobile or Plant Equipment:_____ Manufacturer: _____ Model :_____	The Auditor will verify that the particle produced by the equipment is 1/8 inch maximum or less and that the equipment is of commercial grade. Acceptable deviant tolerance: 1/16 inch.
3.3	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified _____	***PHYSICAL DESTRUCTION OF HARD DRIVES ENDORSEMENT*** Computer Hard Drives are physically destroyed (not wiping or overwriting) in accordance with the Company's standard method of destruction which includes: • Prior to destruction the Company must provide the Customers with a written description of the process for destroying the hard drives. • Serial numbers of all hard drives or CPUs being destroyed for each Customer are recorded, unless the Customer has signed an opt-out agreement. • The log of recorded serial numbers is returned to the Customer upon the completion of the service, unless the Customer has opted out of this requirement. • Hard drives must be damaged to the point where the platters will not spin. Method of Physical Destruction: _____	Auditor will review the Company's written policies and procedures for their standard physical destruction (not wiping or overwriting) of computer hard drives. Auditor will also review verification that the Customer has been notified of the process of destruction. Auditor will also review the serial number recordation log and any opt-out agreements Customers signed.
3.4	Applicant Claims _____ ☐ Not Applicable _____ NAID USE ONLY Verified _____	***NON-PAPER MEDIA ENDORSEMENT*** Non-Paper Media is destroyed in accordance with the Company's standard method of destruction. Any method that deviates from the standard method of destruction must be communicated to the Customer in writing. Types of Non-Paper Media physically destroyed: ☐ Optical Media: _____ ☐ Magnetic Media: _____ ☐ Flash Media: _____ ☐ Other: _____ Method of Destruction: _____	Auditor will review the Company's written policies and procedures for their standard physical destruction of Non-Paper Media. Auditor will also review written policies and copies of documentation provided to the Customer for methods of destruction that deviate from the standard method.

Company Name:_____

		Criteria	Audit Methodology
3.5	Applicant Claims _____ ☐ Not Applicable _____ NAID USE ONLY Verified _____	***PRODUCT DESTRUCTION ENDORSEMENT*** Product Destruction is destroyed in accordance with the Company's standard method of destruction which includes: • Product Destruction is provided in a manner consistent with the company's policies and procedures manual. • The policies and procedures manual must state that customer receiving the product destruction endorsement will be provided a detailed account of the process used to destroy the specific product in advance of the project. Such product destruction agreements must be kept on file for 3 years from the date of the destruction. • Employee Confidentiality Agreements must contain language wherein the employee agrees that products accepted for destruction are to be considered confidential and that removal or use by the employee is a violation punishable by dismissal and subject to possible legal prosecution.	Auditor will review the Company's written policies and procedures for their standard Product Destruction. Auditor will also review verification that the Customer has been notified of the process of destruction with a detailed account of the process used to destroy the product. The notification to the Customer must be kept on file for 3 years from the date of destruction. Auditor will review the employee confidentiality agreements to verify that language stating that the employee agrees that products accepted for destruction are to be considered as confidential and that removal or use by the employee is a violation punishable by dismissal and subject to possible legal prosecution. Has modified policies and procedures to specifically state that clients receiving product destruction services will be provided a detailed accounting of the process used to destroy the specific product in advance of the project, and that such product destruction agreements be kept on file for 3 years from the date of the destruction. (Audit methodology: Reviewed by auditor)
3.6	Applicant Claims _____ ☐ Not Applicable NAID USE ONLY Verified _____	***APPLIES TO PLANT-BASED AND/OR TRANSFER PROCESSING STATION CERTIFICATION ONLY*** The destruction of confidential media must take place within 3 business days from the arrival at the destruction facility. For purges, the destruction of confidential media must take place within 15 business days For Transfer Processing Stations, the confidential material must be transferred to a Plant-based Destruction Operation within 15 business days. If destruction does not occur in the stated timeframe, the Customer must be notified in writing.	Auditor will check the policy and procedures manual to assure that all media is destroyed within the stated timeframe. Exceptions include acts of God, breakdowns or Customer notification to retain media for a longer period.
3.7	Applicant Claims _____ NAID USE ONLY Verified _____	The destruction process has a method of quality control in place to ensure destroyed information is within the stated standards.	Auditor will check policy and procedures manual to assure that there is a quality control procedure in place for ensuring destroyed information is within stated standards.