Louisiana State Police
Non-Criminal Justice Agency Audit FAQ

Why is my agency receiving this audit?

Your agency receives Criminal History Record Information (CHRI) in response to fingerprint-based background checks. Since you are receiving CHRI for non-criminal justice related functions (i.e. licensing and employment), your agency is considered a Non-Criminal Justice Agency (NCJA). The Louisiana State Police (LSP) is responsible for ensuring any NCJA with access to CHRI is compliant with the FBI Compact Council and FBI Criminal Justice Information Services (CJIS) Division policies and procedures. This assessment by the LSP of your organization must be performed minimally once every three years.

Administration of Non-Criminal Justice Functions

1. **Where can I find information that gives my organization authority to access CHRI?**

   The statute authority which provides your organization authority to access CHRI will be listed on your Civil Agency User Agreement.

2. **What if I don't have a copy of the User Agreement between my agency and LSP?**

   This User Agreement is between your agency and the Louisiana State Police giving your agency the authority to have access to Criminal History Record Information (CHRI). If you don't have a copy of your User Agreement, please contact lsp.bcii.ncja@la.gov.

3. **Who should be the NAC within our agency?**

   The Non-Criminal Justice Agency Coordinator (NAC) will be the liaison between your agency and LSP for quality control, dissemination of manuals and other publications, training, audits, and any other matters concerning the use and misuse of CJIS systems. It's not uncommon for the NAC and LASO to be the same person within an agency.

4. **Who should be our agency's LASO?**

   The Local Agency Security Officer (LASO) will be the person ensuring the day-to-day security of the criminal history record information (CHRI) at the agency, as well as developing an enterprise-wide

security program consistent with the CJIS Security Policy. The LASO represents their agency in all matters pertaining to information security. They will ensure your agency's CHRI policies and procedures are enforced, maintain information security documentation, assist the NAC with audits, and keep LSP informed as to any information security needs and problems. It's not uncommon for the NAC and LASO to be the same person within an agency.

5. **How does my agency get set up with Security Awareness Training?**

   To receive access, your agency first must submit your completed User Agreement to LSP. Once submitted and approved, LSP will provide your NAC, as an organization administrator, access to Security Awareness Training using CJIS Online, an industry standard tool for security awareness training. Once your NAC has access to CJIS Online they will be able to create user accounts for organization personnel requiring access to CHRI. Following the user account creation, each respective user would log in to CJIS Online to complete the training and certification exam.

6. **What topics are covered in the Security Awareness Training?**

   There are many topics that are covered in the training depending upon the type of access each person requires. Such topics include:

   - Responsibilities and expected behavior with regard to being in the vicinity of criminal history record information (CHRI) usage and/or terminals.
   - Implications of noncompliance.
   - Incident response (Identify points of contact and individual actions).
   - Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity, etc.
   - Media protection.
   - Protect information subject to confidentiality concerns — hardcopy through destruction.
   - Proper handling and marking of CJI.
   - Threats, vulnerabilities, and risks associated with handling CJI.
   - Social engineering.
   - Dissemination and destruction.

7. **Do all personnel who are required to complete Security Awareness Training have to sign an Acknowledgement Statement of Misuse acknowledging the notification of penalties for misuse of CHRI?**

   Yes. The Louisiana State Police requires each person who has access to CHRI to sign an Acknowledgement Statement of Misuse in addition to completing CJIS Security Awareness Training.

These items must be signed, completed, and retained by your agency NAC for the duration of CHRI personnel access.

8. **Do I need to maintain records of personnel that have access to CHRI?**

   Many agencies require all their personnel to have access to CHRI. If this is the case, then your current list would be your agency roster. If it is only restricted to certain personnel, the list can be the Security Awareness training roster/list you have as that is a requirement to obtain access. An agency can also keep a separate list of individuals that have access in a spreadsheet.

9. **Do I have to review the list of personnel that have access to CHRI?**

   A periodic review of the user list of people who have access to CHRI is important to ensure that the only authorized personnel are accessing CHRI. Many jobs change, people retire, or leave agencies, so it is important to ensure that only those that require access have it.

Applicant Notification and Record Challenge

1. **Do I have to require that an applicant provide a current, valid, and unexpired picture identification document prior to being fingerprinted?**

   Yes. The National Crime Prevention and Privacy Compact Council suggests agencies accept only current, valid, and unexpired picture identification documents as a method of verifying an individual's identity. As a primary form of photo identification, the following documents may be presented by an applicant when being fingerprinted through the LAPS system at Identogo enrollment centers:

   - State-issued driver's license (for those applicants without a driver's license, a state identification card may be presented if the state's identification card standards are the same as for the driver's license.)
   - U.S. Passport or U.S. Passport Card
   - Uniformed Services Identification Card *(Valid Military ID)*
   - Foreign Passport with Appropriate Immigration Document(s)
   - USCIS - Permanent Resident Card (I-551)
   - USCIS - Employment Authorization Card (I-766) *(Valid Work Visa)*
   - Federal, state, or local government agency ID card with photograph
   - U.S. Coast Guard Merchant Mariner Card

2. **Does my agency have to supply applicants with any notification as to what we are using their fingerprints for when completing a background check?**

   Yes, agencies are required to inform the applicant that their fingerprints will be used to check the national criminal history records of the FBI. Title 28 CFR 50.12 (b). The Privacy Statement can be found at https://www.fbi.gov/services/cjis/compact-council/privacy-act-statement.
   Your compliance answer can state that you provide a link to the Compact Council Privacy Act Statement for each user being fingerprinted.

3. **Do I have to capture the applicant's acknowledgement that I supplied them with a privacy statement?**

   Yes, the requesting authority shall maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination; 5 USC 552a (e) (5).

   This means that on an application, Non-Disclosure Agreement, or any personnel record, it must be recorded that you supplied the applicant with the “Privacy Statement” or the link to it. The person’s signature/initials must be captured and kept as part of their personnel file.

4. **Does my agency have to allow the applicant to have the opportunity to challenge the accuracy of the information contained in their criminal history record? Am I under any obligation to advise them as to how to challenge the information?**

   Yes, agencies are required to provide the applicant an opportunity to challenge the accuracy of the information contained in the FBI identification record. Somewhere in the application or in a separate notice, the applicant has to be given the opportunity to challenge the accuracy of their CHRI information if they believe it is inaccurate.

   Agencies are required to advise the applicant of the procedures for obtaining changes, corrections, or updates to the FBI identification record. The subject of a record may direct his/her challenge as to the accuracy or completeness of any entry on his/her record to the FBI, Criminal Justice Information Services (CJIS) Division, ATTN: SCU, Mod. D-2, 1000 Custer Hollow Road, Clarksburg, WV 26306. The FBI will then forward the challenge to the agency which submitted the data requesting that agency to verify or correct the challenged entry. Title 28 CFR 50.12 (b) and Title 28 CFR 16.34

   For challenges/changes to Louisiana criminal history results, individuals must submit a ""Right to Review Authorization Form"" and a ""Right to Review Disclosure Form"" along with fingerprints and the appropriate fees to the LSP Bureau. Individuals can use this record to identify, if applicable, the date

of arrest, the identity of an arresting agency, and disposition information. This criminal history record may only be given to the individual, his authorized representative or his attorney per La. Revised Statute 15:588.

Fingerprint Processing

1. **Does my agency have to include a specific reason in the 'Reason Fingerprinted' field prior to submitting fingerprints for processing?**

   Yes, the Reason Fingerprinted field is important for many reasons. Not only does the Privacy Act of 1974 require that the reason be captured, but entering something in this field will assist whenever your agency is audited. Having a reference in that field will help answer any questions as to why that person's Criminal History was run.

   The Privacy Act of 1974 (Title 5, section 552a) requires that the FBI's CJIS Division keep an accurate accounting of the purpose of each disclosure of a criminal history record. Therefore, all fingerprint-based requests for Criminal History Record Information (CHRI) shall include in the 'Reason Fingerprinted' field an accurate representation of the purpose and authority for which the CHRI is to be used.

2. **What supporting documentation do I need to have to substantiate fingerprint submissions upon request?**

   If requested, your agency will need to provide a valid reason for why you received a criminal history record. An example would be if you require a fingerprint-based background check for employment or licensing, the supporting documentation would be that person’s application.

3. **Why do I need to notify the state when my agency receives a fingerprint response where my agency has no associated application or is unaware why a record response was received?**

   Though it isn't common, should your agency receive a fingerprint response for which you have no associated application, you must contact the State and advise them of this error. Criminal History Record Information (CHRI) may not be disseminated outside the receiving departments, related agencies, or other authorized entities. The State must be contacted to advise them of the erroneous delivery and to obtain procedures for destruction. Title 28 CFR 50.12(b)

Use and Dissemination

1. **Does my agency need to have a written policy to ensure criminal history record information is used only for the official purpose for which it was requested? Should it also contain the use and handling of CHRI? And if so, where can I find information about what it should contain?**

   Your organization must have a written Acceptable Use policy identifying that CHRI shall be used solely for the purpose requested and cannot be disseminated outside the receiving departments, related agencies, or other authorized entities. Public Law 92-544 and Title 28, C.F.R., 20.33 and 50.12(b)

   At the end of this document, there is a section called "Policies Required". You will find information about each policy that is required to be submitted and where you can get further information if needed.

2. **Can I reuse CHRI for a different purpose than what I have entered into the "Reason Fingerprinted" field?**

   Specifically stated, each CHRI record must be used only for the purposes for which it was initially requested.

   Any record obtained under this Compact may be used only for the official purposes for which the record was requested. Each Compact officer shall establish procedures, consistent with this Compact, and with rules, procedures, and standards established by the Council under Article VI, which procedures shall protect the accuracy and privacy of the records, and shall—
   (1) ensure that records obtained under this Compact are used only by authorized officials for authorized purposes;
   (2) require that subsequent record checks are requested to obtain current information whenever a new need arises" Title 34, USC 40316 Article IV

3. **Can I forward CHRI to another agency for them to use it in a separate unrelated application?**

   CHRI can only be used for what it was originally intended to be used for. It cannot be disseminated to another agency to be used for something else or used for something different within your agency. CHRI shall be used solely for the purpose requested and cannot be disseminated outside the receiving departments, related agencies, or other authorized entities. Title 28, C.F.R., 50.12(b)

4. **Can my agency deny employment, a license, or other benefit based on just charges without the final disposition listed on the CHRI?**

   "Officials should not deny the license or employment based on information in the record until the applicant has been afforded a reasonable time to correct or complete the record, or has declined to do so. Title 28 CFR 50.12 (b)"

During the reasonable amount of time an applicant is correcting or completing their record you are allowed to move forward with a different applicant should you wish to do so. During the time the applicant is correcting or completing their record, their application remains open. Once the applicant responds with their challenge results or the reasonable amount of time has expired, it would be the agency's decision to keep the application open or terminate the application process.

5. **Can I release information to the public via a public website, open information request, or press release that confirms or denies the existence of CHRI for a person?**

   CHRI information, even the denial or affirmation that it is in existence is not for use upon request to unauthorized agencies or through public websites. If a person does not have a CHRI record, you cannot state or disseminate that they do not have one. This information cannot be disseminated for any reason to unauthorized personnel. "CHRI shall be used solely for the purpose requested and cannot be disseminated outside the receiving departments, related agencies, or other authorized entities. Title 28, C.F.R., 50.12(b) and (1) Use of criminal history record information disseminated to noncriminal justice agencies shall be limited to the purpose for which it was given. (2) No agency or individual shall confirm the existence or nonexistence of criminal history record information to any person or agency that would not be eligible to receive the information itself." Title 28, C.F.R., 20.21

6. **Can I disseminate CHRI to another agency?**

   No, CHRI cannot be shared outside the receiving agency, with the exception of certain criteria pertaining to the NCPA/VCA (VECHS) and Adam Walsh Act. To determine if your agency falls under one of these exceptions, please contact LSP.BCII.NCJA@la.gov.

7. **Am I allowed to give applicants a copy of their fingerprint-based criminal history record?**

   No. You are allowed to **show** an applicant a copy of their fingerprint-based criminal history record as long as they produce a valid picture identification. If the applicant is going to challenge their record, your agency must provide the applicant instructions on how to obtain their state and/or federal record themselves (Right to Review or FBI Process). You must also advise the applicant that they are not to share their Criminal History Record with other agencies and/or positions they are applying for.

   FBI website for information about record review and challenge:
   https://www.fbi.gov/services/cjis/identity-history-summary-checks

   State website for information about record review and challenge:
   https://lsp.org/about/leadershipsections/support/bcii/fingerprints-and-background-checks/

Outsourcing

1. **What does outsourcing mean and how does it affect my agency?**

   If your agency has been authorized to access, handle, store, and dispose of CHRI by way of your User Agreement, your agency is bound by the User Agreement to ensure only authorized persons have access to CHRI. Anytime your agency has a "contractor" (i.e. another Non-Criminal Justice Agency or vendor) providing access, processing, storage, or disposition services for your agency where the contractor may have access to CHRI or to networks storing CHRI, it is considered "outsourcing" of services. Outsourcing of services could include receiving custodial services where custodial staff can view CHRI on desks or in unlocked storage rooms. It could include receiving services from a municipal IT department where CHRI is stored electronically. Or, it could include contracting with a shredding service to dispose of agency files. Outsourcing occurs in these cases and any other where CHRI could be available to contractor personnel in physical or electronic form while providing an administrative service to your agency.

   Prior to entering into an agreement for services with a contractor, your organization has to have written permission from 1) the State Compact Officer/Chief Administrator or (2) the FBI Compact Officer; and have an executed contract or agreement prior to providing a service provider access to CHRI. Note - The contract shall, at a minimum, incorporate by reference and have appended thereto the National Crime Prevention and Privacy Compact Council Security and Management Control Outsourcing Standard for Non-Channelers.

Security of Criminal History Record Information

1. **What types of controls can I put in place that would ensure that CHRI information is only visible to authorized personnel?**

   At a minimum:
   1. Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI.
   2. Lock the area, room, or storage container when unattended.
   3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.
   4. Follow the encryption requirements found in SC-13 and SC-28 of the CJIS Security Policy for electronic storage (i.e., data at-rest) of CJI.

2. **What is a Physical Protection policy and does my organization need one?**

   The physical protection policy can be part of your media protection policy or a policy on its own. This policy needs to describe where CHRI information is kept, how it is secured, and that access is only granted to those that are authorized to view it.

   Your Physical Protection policy needs to be uploaded into the audit. At the end of this document, there is a section called "Policies Required". You will find information about each policy that is required to be submitted and where you can get further information if needed.

3. **Does my organization have to have a written policy that specifies the procedures for handling, transporting, and storing of physical (i.e. printed) or electronic media by authorized persons?**

   Yes. A media protection policy shall be documented and implemented to ensure that access to digital and physical media in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting and storing media.

   Your Media Protection policy needs to be uploaded into the audit. At the end of this document, there is a section called "Policies Required". You will find information about each policy that is required to be submitted and where you can get further information if needed.

4. **Does my organization have to have a written policy defining how physical/printed criminal history record information (CHRI) is to be destroyed and on what schedule?**

   Yes. This policy is your CHRI Retention and Destruction policy. This policy needs to be specific by stating how long CHRI records (both physical and electronic) are kept, where they are kept, and how they are destroyed.

   Your Retention and Destruction policy needs to be uploaded into the audit. At the end of this document, there is a section called "Policies Required". You will find information about each policy that is required to be submitted and where you can get further information if needed.

5. **Why does my organization have to have a written policy regarding disciplinary action taken for the misuse of sensitive information including criminal history record information (CHRI)?**

   Each agency must have a policy that describes the steps that are taken to discipline someone if they misuse sensitive information that includes CHRI. This policy would be your Disciplinary policy. This policy must contain that any incident of misuse must have notification to the state.

Your Disciplinary policy needs to be uploaded into the audit. At the end of this document, there is a section called "Policies Required". You will find information about each policy that is required to be submitted and where you can get further information if needed.

6. **Does my agency need to have procedures in place to report and document breaches of information or potential security violations to the criminal history record information (CHRI) repository?**

   Yes. To ensure the protection of CHRI, breaches of information and potential security violations must be reported and documented. This policy will be the agency Incident Response policy.

   Your Incident Response policy needs to be uploaded into the audit. At the end of this document, there is a section called "Policies Required". You will find information about each policy that is required to be submitted and where you can get further information if needed.

Technical Security for CHRI

Some organizations may store applicant identification information (e.g. name, date of birth, social security number, etc.) along with **an indicator of the existence of CHRI (e.g. Does a Criminal History Exist? Y/N).** Storing applicant information along with an indication of the existence of CHRI is also considered CHRI.

Storing CHRI on personal computers, network drives, external storage devices, thumb drives, or in the "cloud" is considered **electronic storage of CHRI**. When using any of these devices to store CHRI your organization must adhere to the requirements of the FBI CJIS Security Policy.

If your agency does not store CHRI electronically you can respond N/A to the questions in the Technical Security for Criminal History Record Information Section of the audit. If you do store CHRI electronically, you must answer all of the questions in the Technical Security for Criminal History Record Information Section of the audit. N/A will not be considered a valid response.

If your agency does store CHRI electronically, the following FAQ's are available to assist in understanding the requirements.

1. **If a person retires or changes jobs in my agency and they no longer require access to CHRI, what should I do with their access?**

Each agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The agency shall validate accounts at least annually. Each agency shall grant access to the information systems based on if employees need-to-know/need-to-share the information. Additionally, the agency responsible for account creation shall be notified when:
1. A user's information system usage or need-to-know or need-to-share changes.
2. A user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured.

2. Can I create a generic username and password to get access to CHRI?

There can be no generic usernames or passwords to get into a system where CHRI is kept or accessed. Each person who is authorized to store, process, and/or transmit CJI shall be uniquely identified. A unique identification shall also be required for all persons who administer and maintain the system(s) that access CJI or networks leveraged for CJI transit.

3. Are there specific characteristics that are required for a password?

The CJIS Security Policy is very strict with their password construction. See below for password requirements:
1. Be a minimum length of eight (8) characters on all systems.
2. Not be a dictionary word or proper name.
3. Not be the same as the Userid.
4. Expire within a maximum of 90 calendar days.
5. Not be identical to the previous ten (10) passwords.
6. Not be transmitted in the clear outside the secure location.
7. Not be displayed when entered.

4. Do I need to use encryption to store CHRI electronically?

Applying encryption to electronic CHRI is dependent on a number of factors. When CHRI is kept within the confines of a physically secure area (i.e. a limited access area where users with access have successfully completed a background check and security awareness training), encryption would not be required. However, if CHRI is stored where unauthorized persons may have access, (e.g. organization staff or IT support that have not been vetted) or is stored across networks, (e.g. stored on an organization share drive, stored in cloud storage including Microsoft OneDrive, Google Drive, etc.) encryption must be employed.

CJIS Security Policy Section 5.10 provides guidance on employing minimal standards for transmitting CHRI (SC-13 Cryptographic Protection) and storing CHRI (SC-28 Protection of Information at Rest).

5. **If my agency stores CHRI electronically, do I have to log certain events? And do these logs have to be reviewed at certain times?**

   Yes, when CHRI is stored electronically on network storage, organizations must implement audit and accountability controls to assist in ensuring CHRI is accessed only by authorized users. Audit controls are usually applied at the server level, not individual workstations. Logging helps to establish what events occurred, the sources of the event and the outcome. Auditable events include login attempts, changed passwords, changed permissions, etc., and are more clearly defined in the CJIS Security Policy, Section 5.4 Audit and Accountability (AU), AU-2 Event Logging. Logs also have to be reviewed weekly for inappropriate or unusual activity for security of the system.

6. **Does my organization have to have a written policy and procedure for the sanitizing and disposing of physical or electronic media that contains/contained criminal history record information (e.g. hard drives)?**

   Yes. Each agency has to have a policy that explains how CHRI that is kept on physical or electronic media is disposed of. This will be your Media Sanitation and Disposal policy.

   Your Media Sanitation and Disposal policy needs to be uploaded into the audit. At the end of this document, there is a section called “Policies Required”. You will find information about each policy that is required to be submitted and where you can get further information if needed.

7. **Does my agency need to maintain antivirus and spyware protection and have a patch management process?**

   Yes, accessing CHRI from any device requires a routine patch management process. This ensures that software updates, antivirus, and/or spyware protection are regularly updated to minimize security threats. Your agency (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) shall develop and implement a local policy that ensures prompt installation of newly released security relevant patches, service packs, and hot fixes. The agency shall implement malicious code protection that includes automatic updates for all systems with Internet access. Agencies with systems not connected to the Internet shall implement local procedures to ensure malicious code protection is kept current (i.e. most recent update available).

8. **Is my agency required to maintain a topological network diagram?**

If your agency is storing CHRI or CHRI information electronically, you must maintain a topological network diagram. Review the CJIS Security Policy Appendix C for an example. The organization shall ensure that a complete topological drawing depicting the inter-connectivity of the agency network to criminal justice information, systems, and services is maintained in a current status.

Cloud Storage

1. **Can we use a cloud provider to host/store CHRI and CHRI-related information?**
   When utilizing a cloud provider, controls must be in place to ensure that CHRI is accessible only by authorized persons. Cloud providers may only utilize storage configured within the U.S., U.S. Territories, Indian Tribes, or Canada. Additionally, cloud provider personnel must meet all personnel screening requirements (e.g., security awareness training and have a signed CJIS Security Addendum certification). If the CHRI is unencrypted, the associated metadata shall be protected the same as CHRI and cannot be used for advertising or other commercial purposes.

Policies Required

What policies are required to be submitted with the audit?

1. **The Acceptable Use Policy.** Each agency has to submit a policy to the state of Louisiana outlining their use of CHRI and how it will only be used for official purposes and will not be disseminated outside of the agency to unauthorized entities. Your organization must have a written policy identifying that CHRI shall be used solely for the purpose requested and cannot be disseminated outside the receiving departments, related agencies, or other authorized entities. Public Law 92-544 and Title 28, C.F.R., 20.33 and 50.12(b)

2. **The Physical Protection Policy.** The physical protection policy can be part of your media protection policy or a policy on its own. This policy needs to describe where CHRI information is kept, how it is secured and that access is only granted to those that are authorized to view it. Each agency must have this policy to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

3. **The Media Protection Policy.** This question covers both physical and electronic protection of CHRI. The CJIS Security Policy Section 5.8 assists agencies to document and implement media protection policies and procedures required to ensure that access to electronic and physical media in all forms is restricted to authorized individuals for securely handling, transporting, and storing media. Electronic media is electronic storage media, such as memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash

drives, external hard drives, or digital memory cards. Physical media refers to CJI in physical form, e.g. printed documents, printed imagery, etc.

4. **The CHRI Retention and Destruction Policy.** This policy needs to be specific by stating how long CHRI records (both physical and electronic) are kept, where they are kept, and how they are destroyed. Simply saying they are shredded is not acceptable. You have to state who shreds them, when they are shredded (weekly, monthly), and if they are shredded by an outside company or internal authorized person.

5. **The Disciplinary Policy.** This policy has to specifically state what action your agency will take if a case of misuse of sensitive information or CHRI is found. The policy has to include notification to the state that a misuse has been found and the steps that will be taken to correct the issue.
   Agencies are required to have a written policy on the discipline for misuse of CHRI. The policy should include:
   - Using CHRI for any purpose other than what is allowed by state statute or Federal code is considered misuse.
   - The specific steps your agency will take in the event intentional misuse is discovered
   - Misuse of CHRI can result in loss of access to CHRI, loss of employment and/or criminal prosecution.
   - Misuse of CHRI shall be reported to the state.

6. **The Incident Response Policy.** The Incident Response Policy and Disciplinary Policy are similar. The Disciplinary Policy is based around personnel and what will occur if CHRI is misused. The Incident Response Policy is based around how the agency responds to the misuse or a breach situation. The incident response must cover operational procedures as to how the incident is detected, contained, tracked, documented and who is notified.

7. **The Media Sanitation and Disposal Policy.** The CJIS Security Policy is very specific as to how physical and digital/electronic CHRI is destroyed. This Media Sanitation and Disposal Policy has to specifically state that inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel. The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals.