

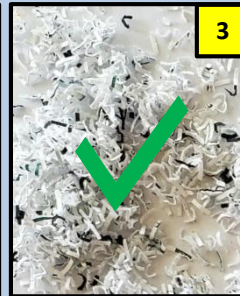
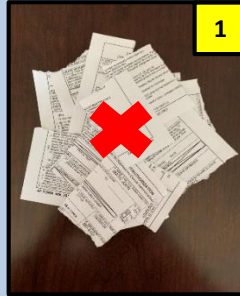
DESTRUCTION OF SENSITIVE UNCLASSIFIED DOCUMENTS

Bottom Line Up Front for AF OPSEC Practitioners

OPSEC practitioners are often asked about specific requirements for destroying paper products containing sensitive data. Exact specifications to meet a requirement of destroying paper “in a manner that would make it difficult to recognize or reconstruct the information” is open for interpretation. Coupled with other mandates to destroy paper products such as medical or privacy act data further clouds the situation. This smart card is designed to break down the various paper destruction requirements to assist OPSEC practitioners with local decisions on paper destruction. Ultimately, our goal is to ensure our adversaries are unable to collect and exploit our sensitive information discarded in trash or recycling bins.

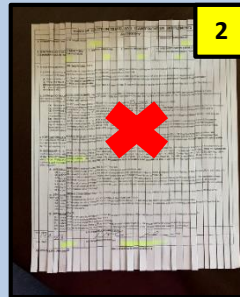
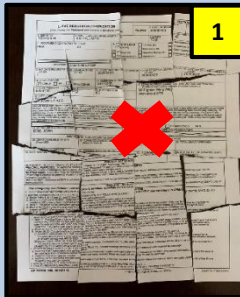
Bad Example: Tearing (1)

- ✗ Difficult to recognize or reconstruct
- ✗ Unreadable, Indecipherable, or Irrecoverable
- Clear indicator the paper is somehow sensitive
- No benefit, not recommend in any way



Bad Example: Strip Shred (2)

- ✗ Difficult to recognize or reconstruct
- ✗ Unreadable, Indecipherable, or Irrecoverable
- Clear indication data on the paper is sensitive
- Strip shredding is better than no shredding



Good Example: Cross Cut Shred (3)

- ✓ Difficult to recognize or reconstruct
- ✓ Unreadable, Indecipherable, Irrecoverable
- ✓ Very effective OPSEC countermeasure

Health Insurance Portability & Accountability Act (HIPAA)

AFI 41-200: HIPAA

- 3.9.2. Destruction. ...the documents must be properly destroyed and disposed of by rendering records or data unusable, unreadable, or indecipherable. (T-0)
- 3.9.3.2. PHI in paper format should be immediately shredded. If the PHI cannot be immediately shredded, it will be placed in a locked, secure area until it can be destroyed. (T-0) PHI must not be disposed of in the regular garbage or recycle bins. (T-0).

Privacy Act Information

AFI 33-332: Air Force Privacy Act Program

- 7.3.1. Destroy by any method that prevents compromise, such as tearing, burning, or shredding, so long as the personal data is not recognizable and beyond reconstruction.
- 7.3.3. Dispose of paper products through the Defense Reutilization and Marketing Office (DR&MO) or through activities who manage a base-wide recycling program.

DOD 5400.11-R: DoD Privacy Program

- C1.4.3.1. Dispose of records containing personal data so as to prevent inadvertent compromise. Disposal methods are those approved by the Component or the National Institute of Standards and Technology. For paper records, disposal methods, such as tearing, burning, melting, chemical decomposition, pulping, pulverizing, shredding, or mutilation are acceptable.
- C1.4.3.2. Disposal methods are considered adequate if the personal data is rendered unrecognizable or beyond reconstruction.

Controlled Unclassified Information (CUI)

Unclassified data associated with a law, regulation, or government-wide policy and identified as needing safeguarding is considered CUI. Note: Information identified in an organization's Critical Information & Indicators List (CIIL) falls into a specific category of CUI; see <https://www.archives.gov/cui/registry/category-detail/opsec> for more information.

AFI 33-364: Records Disposition – Procedures and Responsibilities

- 5.10.2. Destroy...sensitive unclassified information (to include Privacy Act, FOUO, privileged, or proprietary information) and personal records that, according to responsible officials, contain information that might be prejudicial to the interests of the government, public, or private individual by any means approved for classified information or by any means that would make it difficult to recognize or reconstruct the information. Methods and equipment used to destroy classified information include burning, crosscut shredding, wet pulping, chemical decomposition, or pulverizing. Only use equipment specified on the National Security product list.

Title 32 CFR Part 2002: CUI

- **(f)(2)** When destroying CUI, including in electronic form, agencies must do so in a manner that makes it unreadable, indecipherable, and irrecoverable. Agencies must use any destruction method specifically required by law, regulation, or Government-wide policy for that CUI. If the authority does not specify a destruction method, agencies must use one of the following methods:
 - **(i)** Guidance for destruction in NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, and NIST SP 800-88, Guidelines for Media Sanitization (incorporated by reference, see § 2002.2); or
 - **(ii)** Any method of destruction approved for Classified National Security Information, as delineated in 32 CFR 2001.47, Destruction, or any implementing or successor guidance.

DoDI 5200.48: CUI

- 4.5 (a) When destroying CUI, including in electronic form, agencies must do so in a manner making it unreadable, indecipherable, and irrecoverable. If the law, regulation, or government-wide policy specifies a method of destruction, agencies must use the method prescribed.

DoDD 5210.83: DoD Unclassified Controlled Nuclear Information (UCNI)

- 6 (c) Non-record copies of DoD UCNI shall be destroyed by shredding or burning or, if the sensitivity or volume of the information justifies it, in accordance with the procedures specified by DoDM 5200.01-V3 (Reference (1k)) for classified information. Record copies of DoD UCNI shall be disposed of in accordance with the DoD Component's record management regulations.

Additional References

The following additional resources are provided to enhance your understanding of how to protect and destroy sensitive information.

- **Information Security Oversight Office CUI Notice 2019-03**
<https://www.archives.gov/files/cui/documents/20190906-cui-notice-2019-04-private-sector-entities.pdf>
- **NIST Special Program 800-88, rev. 1**
<http://dx.doi.org/10.6028/NIST.SP.800-53r4>
- **National Security Agency Evaluated Products List (EPL)**
<https://www.nsa.gov/Portals/70/documents/resources/everyone/media-destruction/NSAEPL%20Paper%20Shredder%2011-06-18.pdf?ver=2018-12-12-122128-333>
- **Executive Order 13556: Controlled Unclassified Information**
<https://www.federalregister.gov/documents/2010/11/09/2010-28360/controlled-unclassified-information>
- **AFI 10-701, Operations Security (OPSEC)**
https://static.e-publishing.af.mil/production/1/af_a3/publication/afi10-701/afi10-701.pdf

Parting Thought

Destroying papers with sensitive information is bigger than just OPSEC. Other mandates for medical and privacy act data should also be considered and any destruction level should meet requirements for all.



Air Force OPSEC Support Team (AF OST)
Joint Base San Antonio – Lackland AFB
DSN 312-945-3952/2667
Commercial 210-925-3952/2667
AF.OST@us.af.mil
www.facebook.com/AirForceOST/

Remember: Better SHRED than READ!