Describing a data entity attribute.

ATTRIBUTE\_SENSITIVITY\_TYPE M ATTRIBUTE

**Mandatory**: always required

Attributes:

* **Classification:** 1=Unclassified, 2=CUI, 3=Confidential, 4=Secret, 5=Top Secret, 6=Special, 7=TBD (Value type?)
* **Creation date:** Month day and year of creation; **defaulted:** ingest date to the system, if exact date of creation is not known (Value type?) Use ISO 8601 date format: YYYYMMDD.
* **Creator**/originator/owner: Person who created it, organization that generated it, the classified document owner from which the information was abstracted. (Obligation?)
* **Protection:** Classification Value/Obligation + Creation date. (Determines protection controls, duration and reviews) (Obligation?)

ATTRIBUTE\_SENSITIVITY\_TYPE M ATTRIBUTE

Encryption of sensitive data shall be accomplished by transmitting the data using a secure method (i.e. SSL, HTTPS, SFTP, etc.) and by relying upon the encryption capability built into the computer’s operating system or hardware for the specified security need of the information. Moving to Post Quantum Encryption at the earliest opportune date.

Establish a system of control measures, to assure that access to information is provided to authorized persons. The control measures shall be appropriate to the environment in which the access occurs and the nature and volume of the information.

NIST SP 800-171r3 defines current requirements for CUI.

*Control level* is a general term that indicates the safeguarding and disseminating requirements associated with CUI Basic and CUI Specified.

Decontrolling*.* occurs when an authorized holder, consistent with this part and the CUI Registry, removes safeguarding or dissemination controls from CUI that no longer requires such controls. Decontrol may occur automatically or through agency action. See [§ 2002.18](https://www.ecfr.gov/current/title-32/section-2002.18).

Automatic declassification**.** The referral process for records subject to automatic declassification entails identification of records containing classified information that originated with other agencies or the disclosure of which would affect the interests or activities of other agencies.

Migration

Migration processes are still in a developmental phase, but there is some ongoing data migration, there is a need to backup and safeguarding the information. This plan should include geographically separate storage locations. Recovery and back up plans. Safeguarding from unauthorized access and corruption. With the advent of quantum computers, long-term security of individual data items is a concern and migration from current cryptographic protections should occur to Post Quantum Cryptography.