SPIRION

Spirion Extensions

Locate & Protect Controlled Unclassified Information (CUI) on Workstations & Servers for CMMC Compliance

Using Spirion to Locate and Protect Controlled Unclassified Information (CUI) on Workstations and Servers for CMMC Compliance

Introduction

Controlled Unclassified Information (CUI) is an umbrella term that represents a particular kind of sensitive data: data created by the U.S. federal government or developed on its behalf and that merits special protection against exposure. Under this umbrella are categories such as:

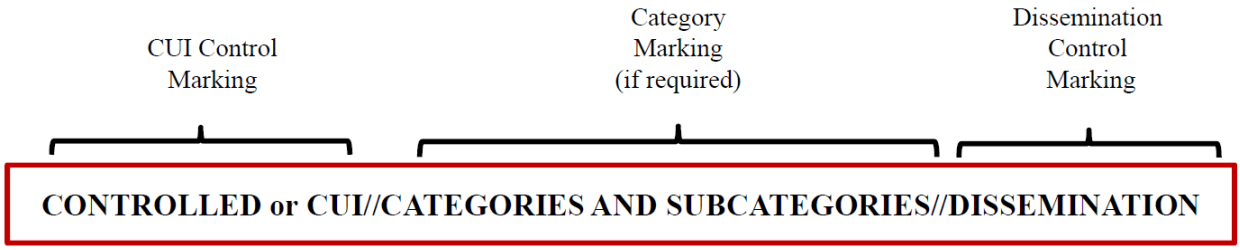
- Controlled Technical Information (CTI), technical data that is used on a day-to-day basis by aerospace and defense contractors to design, build, service, and repair a wide range of aircraft, ships, vehicles, systems, infrastructure, and other components of U.S. national defense.

- Export Controlled, technology that if exported, could reasonably be expected to harm U.S. national security, such as “dual use” technology, items on the national munitions list, and sensitive nuclear technology information.

- Critical Energy Infrastructure Information, which is specific engineering, vulnerability, or detailed design information about proposed or existing critical power grid infrastructure that could be used to attack it.

Even though, by definition, CUI is unclassified (i.e., not “Secret” or “Top Secret”), loss by, or exfiltration from, a defense contractor can substantially harm the defense posture of the United States and its allies.

U.S. government rules for protecting CUI include marking documents and other information with indicators of a protected status. The National Archives and Records



Administration (NARA) issued a handbook on marking best practices in 2016. The handbook cites the following format for proper markings:

For example: **CUI//SP-CTI//FEDCON**
In other words, a document (such as a schematic) with this marking is considered to be controlled, is protected as controlled technical information, and dissemination is limited to federal agencies and their contactors.

A new cybersecurity regime designed to protect CUI, the Cybersecurity Maturity Model Certification (CMMC)[1], was introduced in January of 2020 by the U.S. Department of Defense. Its use will be mandatory for all defense contractors, starting sometime late in 2020. As a result, the ability to locate and protect CUI in a company's information ecosystem is imperative if it wishes to obtain new government contracts.

A Short History of CUI and Laws Protecting It

Before the concept of CUI was introduced in 2008, documents that contained sensitive defense information such as schematics, reports, and other technical data were marked with an array of acronyms that were indicative of its protected status, such For Official Use Only (FOUO) and Sensitive But Unclassified (SBU). According to some sources in the defense establishment, there were roughly 100 different such acronyms, leading to inconsistent protection for technical data.

To remedy this problem, Executive Order (EO) 13556 was issued in November of 2010 by the Obama administration. The EO placed NARA in charge of collecting CUI categories from the many federal government agencies and creating a master list. The National Institute of Standards and Technology (NIST) was placed in charge of developing data protection standards for CUI, which were eventually published as NIST Special Publication (SP) 800-171.

[1] See Office of the Under Secretary of Defense for Acquisition & Sustainment Cybersecurity Maturity Model Certification, found at https://www.acq.osd.mil/cmmc/index.html.

Finally, the U.S. Department of Defense was charged with developing contract requirements for defense contractors that incorporated CUI and SP 800-171. Those requirements manifested in the Defense Federal Acquisitions Regulations Supplement (DFARS) 252.204-7012 - *Safeguarding covered defense information and cyber incident reporting* (referred to as DFARS 7012).[2] Defense contractors and their subcontractors were required to self-certify by December 31, 2017 to be in compliance with the mandates of DFARS 7012 if they wished to bid on or otherwise participate in Department of Defense contracts.

However, weaknesses in the implementation of DFARS 7012 led the Department of Defense to promote a new program using third party assessors to certify that a contractor could meet a given set of cybersecurity mandates. That program, the Cybersecurity Maturity Model Certification (CMMC), was published in January of 2020. By late 2020, all defense contractors, including their subcontractors, will have to be certified by a third party as compliant with a particular gradation within the CMMC (most likely Level 3), **and such compliance hinges on their ability to identify CUI and implement controls to protect it as directed by DFARS 7012**.

The Problems That Spirion Solves

Featuring a proprietary set of technologies, Spirion can effectively identify CUI throughout an enterprise by searching text and images for phrases, words, and acronyms that are indicative of CUI, such as:

- ITAR (International Trafficking in Arms Regulations)
- EAR (Export Administration Regulations)
- USML (United States Munitions List)
- NOFORN (no transfers to non-U.S. persons)
- FOUO
- SBU
- DFARS

It can also look for program names:

- JSTARS
- F-35
- V-22

Finally, it can look for any of the CUI categories delineated by NARA, including:

- CTI (Controlled Technical Information)
- NNPI (Naval Nuclear Propulsion Information)
- DCNI (Unclassified Controlled Nuclear Information – Defense)

[2] 48 CFR § 252.204-7012

Spirion's precision is achieved via Branching Validation processes comprised of dozens of predefined and linear classifiers, procedural validators (when searching data this means search results can be precisely validated using tree traversal so that the results of early validations can determine whether any and which additional validations are executed), checksums, Boolean logic formulas, decision trees, exact data matches, dictionaries, and an optional user-defined rule builder. In doing so, Spirion avoids the high false positive rate (and associated frustration) associated with pure pattern matching, "free" search tools.

Spirion can also assist in compliance with CMMC via its data classification capabilities. For example, upon locating CUI, Spirion can insert multiple appropriate metadata labels, such as **CUI//SP-NNPI** or **Class 3 – DFARS** or any number of other labels (e.g., **PII** or **Proprietary & Confidential**). Those labels can also be read by allied technology, such as data loss prevention (DLP) and next-generation firewalls (NGFW), which can make decisions according to the contractor's data classification policy (deny movement, deny uploads, etc.).

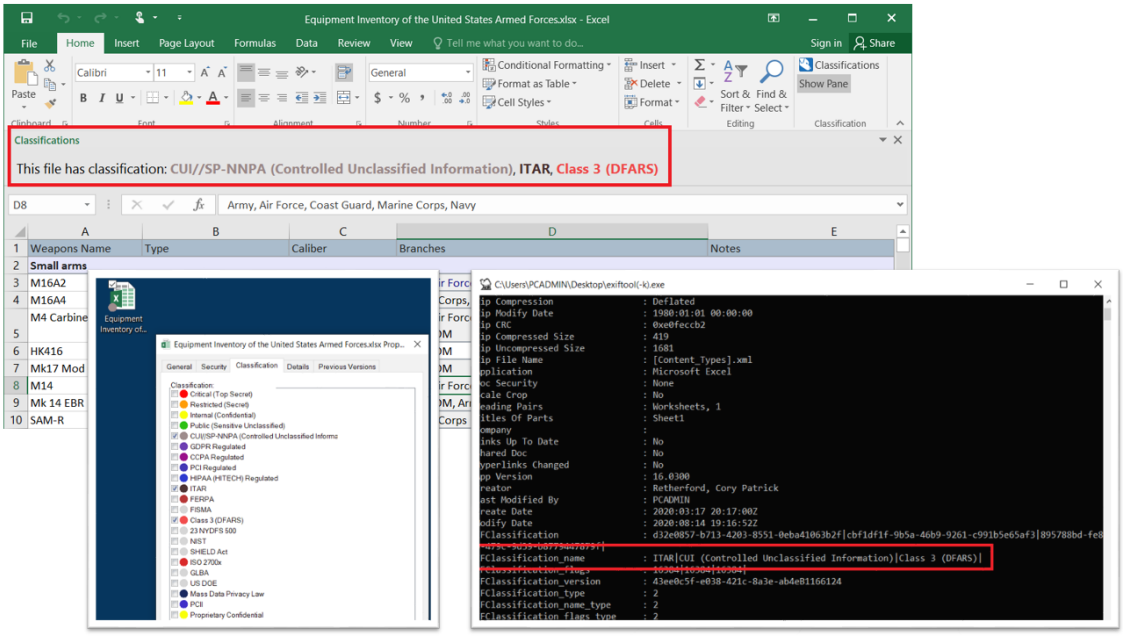


Figure 1. Spirion can embed multiple labels into a document or file, enabling effective protection of CUI, personal information, and intellectual property.

Data Protection Laws Implicated

Legal authority for the protection of CUI and the mandates to develop a program to protect it stem from EO 13556. That order sent into motion three government bodies:

- NARA, which gathered and organized the many categories of CUI into a CUI registry pursuant to 32 C.F.R. Part 2002.
- NIST, which published guidelines on the implementation of cybersecurity controls, principally Special Publication 800-171; and

- DOD, which published the contract clause that became a condition for a defense contractor accepting a contract that incorporated CUI, DFARS 7012.

Note that none of the forgoing represents, *per se*, a cybersecurity statute; rather, collectively it is a function of the DOD's purchasing power. The promotion of the CMMC program is a manifestation of that power.

Requirements

This process requires the following prerequisites in which to make this process possible. These include:

- Current versions of the SDM product(s).
- All Files "SDD".
- Search "Policy" creation.

Important Notes

Controlled Unclassified Information (CUI) will be specific to the program and encompass search terms such as phrases, words, and acronyms that are indicative of CUI such as **CUI//SP-CTI**.

From within Spirion you can create or use customized templates (Sensitive Data Definitions) to locate the CUI types of data using the below steps.
Additional information is available in an article on the Spirion Customer Support Portal's Knowledgebase: Controlled Unclassified Information (CUI) Sensitive Data Definitions | Spirion Portal | Spirion

There are a number of SDD's to choose from which include the CUI NARA categories, markings and groupings, select from the available templates:

- Categories
- Banner Marking: Specified Authorities
- Category Marking
- Organizational Index Grouping

The following Sensitive Data Definitions are available from within the Marketplace Sensitive Data Definitions offerings for Sensitive Data Manager (SDM).

Individual Controlled Unclassified Information SDD's.

- CUI – Categories
    - **CUI - Categories SDD.zip**
- CUI – Banner Marking: Specified Authorities

    - **CUI - Banner Marking_ Specified Authorities SDD.zip**
- CUI – Category Marking
    - **CUI - Category Marking SDD.zip**
- CUI – Organizational Index Grouping
    - **CUI - Organizational Index Grouping SDD.zip**

All the combined CUI conditions combined into a single SDD.

CUI - Controlled Unclassified Information Markings (NARA) SDD.zip

- CUI – Categories
    - Example - Accident Investigation
- CUI – Banner Marking: Specified Authorities
    - Example - CUI//SP-AIV
- CUI – Category Marking
    - Example - AIV
- CUI – Organizational Index Grouping
    - Example - Law Enforcement

Banner and Category Marking only SDD (NARA).

CUI - Banner and Category Markings (NARA) SDD.zip

- CUI – Banner Marking: Specified Authorities
- CUI – Category Marking

CUI Near Banner Marking: Specified Authorities SDD.

CUI - CUI with Banner Marking_ Specified Authorities SDD.zip

- CUI – CUI with Banner Marking: Specified Authorities
    - Most common CUI category or marking search used.
        - Example - CUI Near SP-AIV