

Seamless Transition to CUI Markings

Meeting Controlled Unclassified Information (CUI) Requirements

The Controlled Unclassified Information (CUI) program, originally implemented in 2018, standardizes the way all government agencies and military entities handle unclassified information that requires safeguarding. It clarifies and limits what kinds of information to protect, defines what is meant by “safeguard,” reinforces existing legislation and regulations, and promotes authorized information-sharing.

While it is critical to set standardized controls for the way information is handled, the process of implementing CUI markings across agency data is complex, time-consuming, and sometimes unclear. Yet all agencies are required to use CUI markings on all data that is not classified.

To avoid widespread confusion, it is important to ensure that all agencies use the same procedures to implement the CUI markings. Fortra’s Data Classification Suite (DCS), a recognized leader in document marking and metadata technologies, offers a fully customizable data protection solution that helps address the many different CUI program requirements of U.S. federal departments and agencies.

DCS integrates CUI markings with existing Classified National Security Information (CNSI) markings to provide users with a fully integrated approach to document markings. Metadata collection is also provided so metadata can be integrated with protections required under NIST 800-53 and 800-171 in federal and industry systems.

The DCS solution supports the following:

- All required markings
- Predefined lists of appropriate markings to aid in user decision-making
- Automatic capture of metadata that facilitates appropriate protection of information

ACME - Document for review

Please select CUI Category-Subcategory

CUI*

- CONTRACT Specified - Privacy: Contract Use
- CTI Specified - Controlled Technical Information
- GENETIC Specified - Privacy: Genetic Information
- EXPT Specified - Export Control
- HLTH Specified - Privacy: Health Information

*One or more selections are required

OK Cancel

DCS Provides Quick-Pick Lists To Choose and Apply All Required CUI Markings

The DCS solution, when integrated with employee training programs, dramatically shortens CUI program training time. Employees learn the important markings for their mission, and DCS provides quick-pick lists to choose and apply all required markings.

Dissemination controls are also included in the DCS marking and metadata process. Automated dissemination of information protects data from unauthorized users, metadata that identifies categories of authorized users is captured when employees mark documents in accordance with government policies. This metadata can be used by federal systems to ensure that sensitive information is not shared beyond the defined authorized users.

Fully Customizable

Customize the user experience for each of your user groups. Because federal users have unique needs often down to the unit level, the DCS solution provides small and large user groups with the views, markings and prompts needed for a specific mission.

Integration With CNSI Requirements

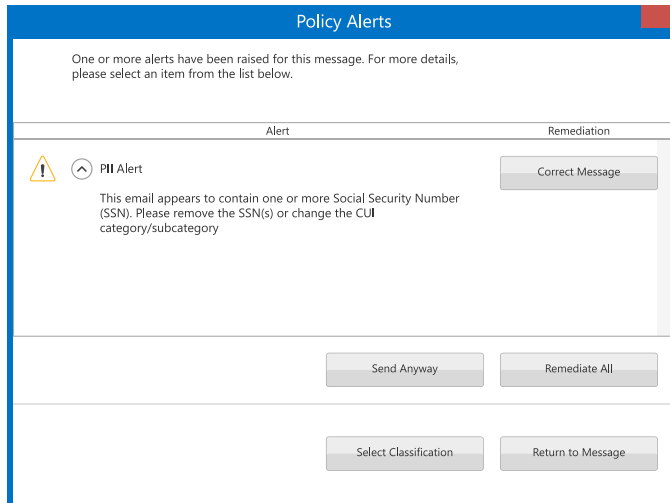
The DCS marking application is a proven marking tool for classified information. The implementation of CUI markings by federal departments and agencies will be unique for each agency and unit mission. Some agencies may not apply CUI markings when a document contains classified information. Other agencies will mark both the classified and controlled information within the same document. The DCS solution can meet all of these individual needs.

DCS provides a customizable application that allows federal agencies to decide what markings to apply. As standards and requirements change during the implementation period, DCS can be changed and modified on-the-fly to ensure that mission priorities continue to be met even during changes in policies and standards.

Optional Advanced User Decision Support With Machine Learning

Set up your systems to automatically identify sensitive information that requires markings and protection with DCS, supported by a machine learning algorithm. While machines will not replace the intuition of human users, prompting users when they create a document can help ensure that the required protection markings are added to that document.

For example, personally identifiable information (PII) is ubiquitous in government documents and may not always be recognized by users. Fortra's DCS Intelligent Protection can be trained to identify such information and warn users that it may require CUI markings. It can also identify data that is not authorized for transmission on the system where it has been stored or posted. In addition, DCS can help prevent information that is limited to government users from being sent to commercial URLs.



DCS Open Architecture: Setting The Stage For Advanced Applications

DCS solutions empower organizations to secure, govern, classify, and identify their data with the only intelligent policy engine that simultaneously manages multiple regulations AND user-defined tailored organization rules. The DCS solution is more open, more intelligent and more flexible, leading to more effective cybersecurity programs, greater productivity, and reliable performance.



About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.