FORTRA™

SOLUTION BRIEF (Fortra)

NIST SP 800-171 and CUI

Meet Compliance Requirements To Protect Controlled Unclassified Information

Originally imposed in 2017, NIST Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, requires all current U.S. Department of Defense contractors to be be compliant with DFARS Part 252.204-7012. Other executive branch agencies may also require nonfederal entities, including contractors, to follow NIST SP 800-171 when sharing CUI through contracts, memorandums of understanding, or acquisition rules.

NIST SP 800-171 provides a standardized set of requirements for all CUI security needs, tailored to nonfederal systems. Data Classification Suite (DCS) solutions help contractors comply with these requirements, especially in the areas of CUI marking, safeguarding, training, and auditing.

Recognize And Apply CUI Markings

Organizations may receive information marked as CUI, or need to apply CUI markings based on original or derivative sources. DCS recognizes government-applied CUI markings and provides users with the tools to add or change markings if authorized. The CUI marking scheme can also be configured to exist alongside other marking schemes, such as those for ITAR and EAR export control. With the option of advanced user decision support using Maching Learning, systems can also be set up to automatically identify sensitive information through Fortra's DCS Intelligent Protection.

Safeguard Cui From Disclosure

It is the responsibility of the CUI holder to honor CUI markings and ensure adequate protection. DCS assists users by clearly identifying CUI in email and documents, along with any associated handling restrictions. DCS also helps safeguard CUI by applying special handling rules and controls, including recipient clearance checking, redaction of sensitive information, and automated encryption.

Raise CUI Awareness

NIST SP 800-171 requires users to be aware of CUI security risks and to know the applicable policies, standards, and procedures to protect the information. DCS provides targeted, real-time security education as users work with CUI in email, documents, and files. These alerts and messages increase awareness and accountability for protecting CUI.

Raise Audit User Activity

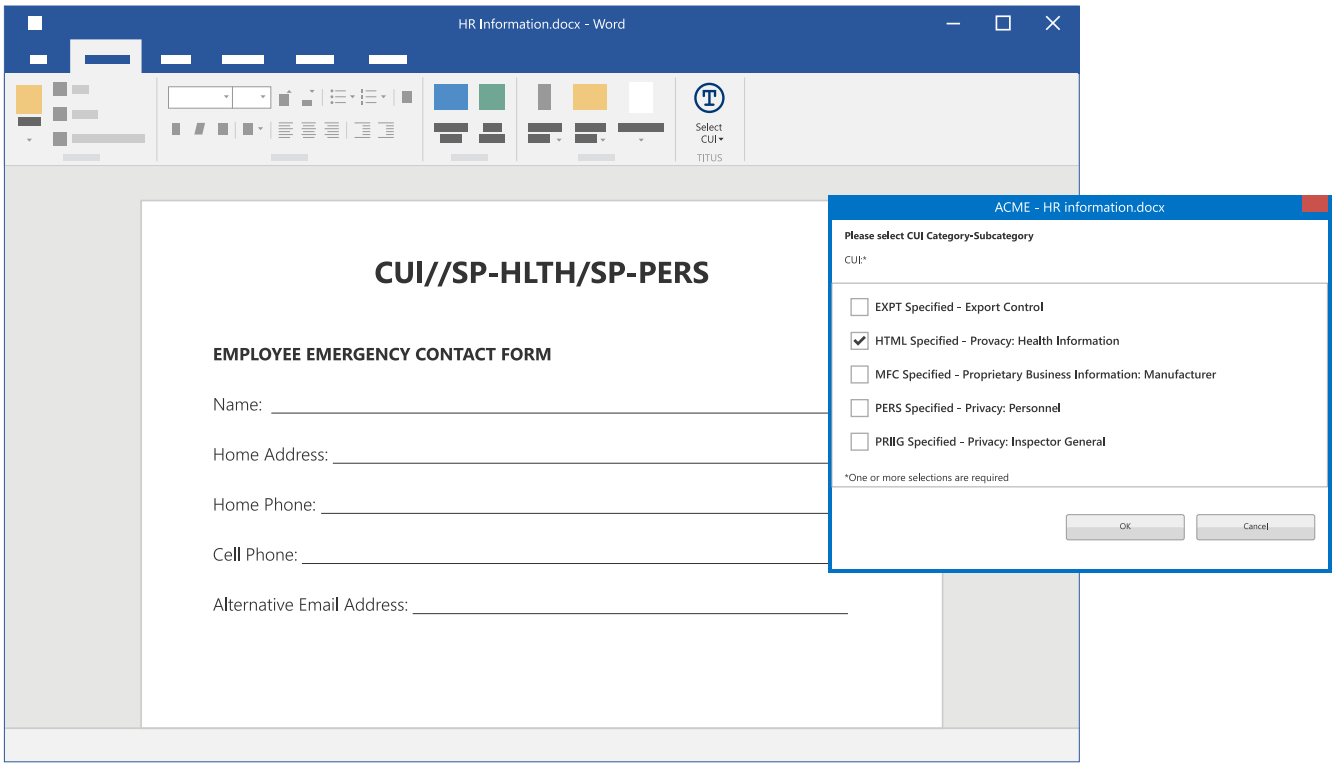
Organizations must be able to track unlawful, unauthorized, or inappropriate CUI activity. DCS logs the actions of individual users as they handle CUI and other sensitive information in email, documents, and files. These logs can be used to create detailed reports on user activity, helping to hold users accountable for their actions.

Protect CUI Across Boundaries

CUI must be protected as it is created, shared, and stored. DCS applies metadata to unstructured data so that other security solutions can identify and protect CUI in email, documents, and files. This metadata can be used by existing technology investments, such as DLP, CASB, encryption, archiving, and guards and gateways.

DCS Helps Address Key NIST SP 800-171 Security Requirements.

- Access control
- Awareness and training
- Audit and accountability
- Media protection
- System and communications protection



DCS recognizes and applies CUI markings

FORTRA™

Fortra.com

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.