titus
by HelpSystems

SOLUTION BRIEF *(Data Classification)*

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. Titus 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. Titus 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 Titus Intelligent Protection.

Safeguard CUI from disclosure

It is the responsibility of the CUI holder to honor CUI markings and ensure adequate protection. Titus assists users by clearly identifying CUI in email and documents, along with any associated handling restrictions. Titus 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. Titus 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. Titus 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. Titus 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.

Titus helps address key NIST SP 800-171 security requirements.

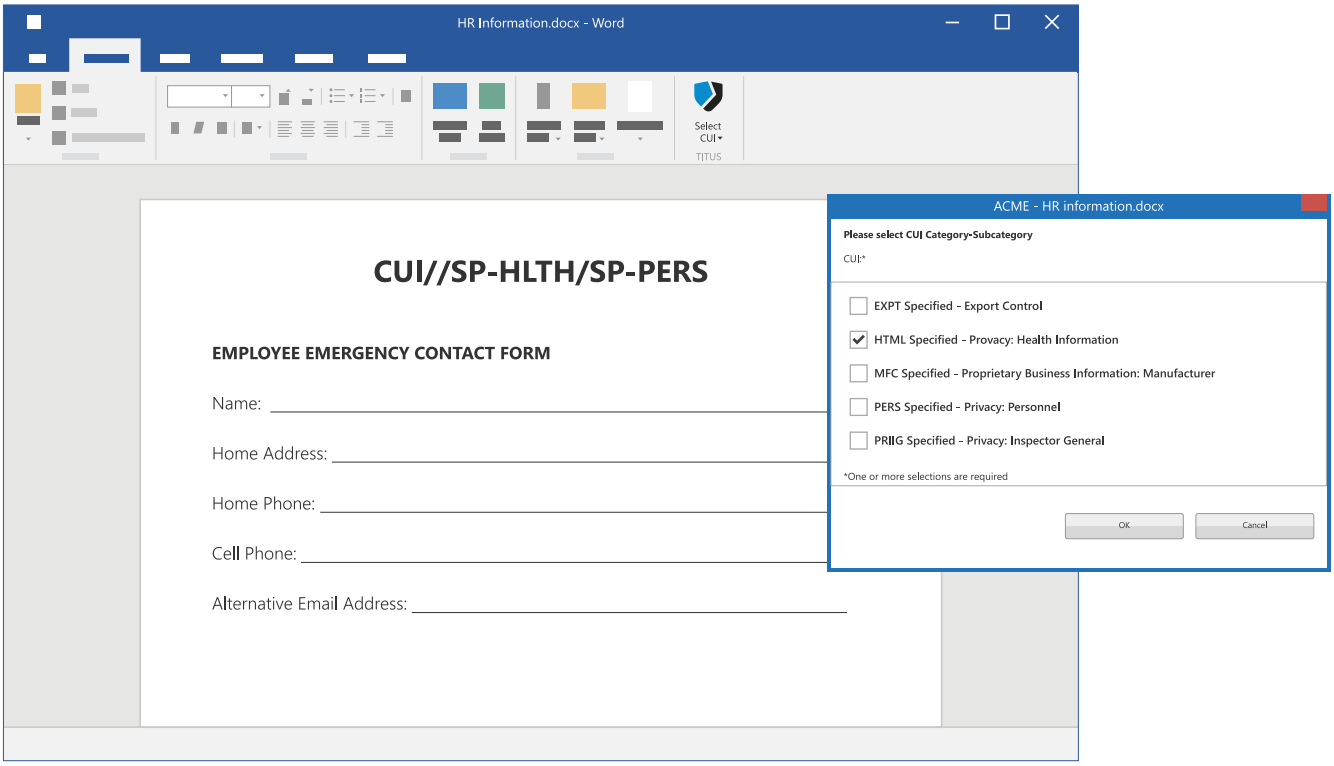
Access control

Awareness and training

Audit and accountability

Media protection

System and communications protection



Titus recognizes and applies CUI markings

titus
by HelpSystems
www.titus.com

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.