

Sentris®

Streamlining CUI Compliance and Securing Sensitive Information

Sentris®: The Smarter Way to Manage CUI Policies and Markings

The Controlled Unclassified Information (CUI) is defined as information created by the government, or an entity on behalf of the government, that is unclassified, but needs safeguarding.

Per NIST Special Publication 800-171, “*The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully conduct its assigned missions and business operations.*”

Ensuring compliance with CUI security requirements to prevent inadvertent disclosure of CUI is a challenge many organizations face. Sentris® can ease the marking of CUI as well as custom organization (i.e., proprietary and most private) classification rules in a Sentris® environment. Sentris® rule sets and other administration utilities provide organizations the flexibility and scalability to modify CUI enforcement as information or organizational classifications and policies evolve.

Enables Information Sharing, Protection and CUI Policy Compliance

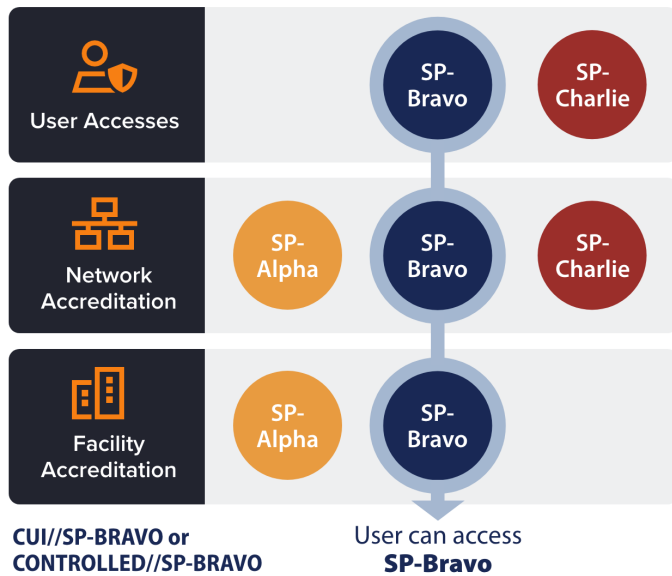
Sentris® is a Microsoft Windows based platform, developed by MANTECH, for implementing attribute-based security classification services within network environments that require a high degree of data security and confidentiality. Sentris® provides users with easy-to-use tools to label and secure content using common applications, such as Microsoft Windows, Office, SharePoint, Skype for Business and Outlook. Sentris® is unique in its capability to control access to data based on three criteria:



- Who is accessing the data (user security accesses)?
- Where is the data being accessed from (facility clearances)?
- What system is the data being accessed from (network accreditations)?

This innovative approach to criteria-based access control allows agencies to manage access to information easily and efficiently in complex, high-security environments where traditional access control mechanisms are ineffective and cumbersome.

SENTRIS® Security Paradigm

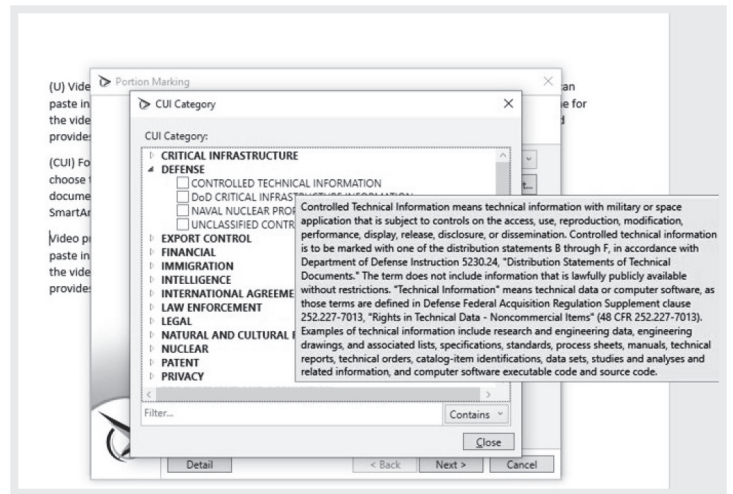


Supports Key U.S. Government Information Sharing Initiatives and CUI Security Requirements

Sentris® is designed to support the DoD Risk Management Framework (RMF) Baseline + Accessibility Overlay requirements to prevent inadvertent disclosure of restricted information. Sentris® powers ultra-secure marking of critically sensitive designated information as well as custom organization classification rules. While Sentris® is designed to meet or exceed the confidentiality requirements specified for classified networks, it is equally customizable to meet the security requirements for CUI networks. Highly flexible and scalable, Sentris® can accommodate the data classification needs of virtually any government agency.

Sentris® enables organizations to:

- Define the types of sensitive information that are authorized to be processed on Microsoft Windows networks.
- Authorize users, facilities and networks for specific classification levels, handling caveats and control markings based on your metadata definitions.
- Provide users with utilities to associate classification labels with the information that they create consistently across applications and functions.
- Control access to information based upon its associated classification label.
- Establish trusted connections with other organizations to allow sharing of classified information across organizational boundaries.



Provides Rich Functionality in a User-Friendly Platform for Accurate CUI Data Classification and Sharing

With Sentris®, users can easily comply with CUI labeling requirements without significant training. Sentris® can be configured to automatically scan documents for keywords and alert the user to the presence of potential CUI data. Additionally, Sentris® can require a document to be marked prior to saving or printing. If a user is sending an email that contains CUI in the subject, body or an attachment, Sentris® will require the email to be marked before it can be sent.

Sentris® adds controls to the ribbon and menu items in standard Microsoft Office applications so users can insert document labels (CUI Banner Markings) in the headers and footers using marking dialogs; print with a custom coversheet; search for sensitive words in the file; and readily mark portions of text, such as paragraphs, figures and tables.

Sentris® simplifies complex data classification, making it easier to share information securely and allowing system security officers to enforce user and organizational access control. By ensuring consistent labeling of classified information and CUI, it accelerates replacing “need to know” with “responsibility to provide.”

Intelligent Governance for CUI Environments

Implement critical CUI data protection policies with confidence. Sentris® is a turn-key solution that integrates with your existing infrastructure to enforce marking and access governance. Join a community of over 50 government and private organizations and 120,000+ users who trust Sentris® for secure data handling.

In business more than 57 years, MANTECH excels in cognitive cyber, AI, data collection & analytics, enterprise IT, systems engineering and software application development solutions that support national and homeland security.

LEARN MORE - www.MANTECH.com/commercial-services

Chris Hassett, Sr. Executive Director, Commercial Software & Services | commercial.services@MANTECH.com

