titus
by HelpSystems

Controlling CUI: The Role Of Data Classification In Meeting U.S. Government Requirements

Including

- What is CUI?
- The evolution of the rule
- The case for compliance
- The nuts and bolts of CUI
- The principles of data classification
- The 5 steps to effective CUI classification

Introduction

After years of deliberation, the U.S. government's National Archives and Records Administration (NARA) has released more details of its regulation for the protection framework of Controlled Unclassified Information (CUI). The rule is designed to safeguard government data that has not been assigned as confidential or secret, but which should not necessarily be made public, as it is shared between different government and commercial entities. At the heart of the framework is a requirement for all CUI to be labelled with appropriate visual markings that indicate to downstream parties how it should be treated.

The framework is primarily designed to control the dissemination of CUI within federal agencies and departments, but also covers information when it resides in non-federal information systems and is handled by non-federal organizations. This is likely to extend to commercial contractors and suppliers that do business with the U.S. government – any of which may be required to receive, store, process and disseminate CUI (and in some cases produce content that contains it).

The Evolution Of The Rule

Efforts to break down information silos within the U.S. government and improve the sharing of data have led to an increase in the number and diversity of people who access and work on CUI. For instance, a department that manages water services might be sharing details of a pipeline's location with transport agencies and engineering companies to inform the planning of roadworks. This has diluted the control that federal government has over its CUI.

Combined with the rapid adoption of the Cloud, the explosion of different platforms and devices, increased mobile working and the evolving security threat, this trend led to an urgent need for a standardized classification framework that would protect CUI without impeding the authorized sharing of it.

Due to the numerous different types of information passing between government entities and commercial organizations it has taken seven years to develop an appropriate rule for classifying CUI. We now have a uniform framework that pulls together what was once a piecemeal, confusing and inconsistent approach, making the appropriate treatment of CUI clearer, more efficient and easier to apply.

What Is CUI?

Controlled Unclassified Information (CUI) is data that is created or possessed by or on behalf of the federal government which is not classified, but is either required or allowed to be protected by law, regulation or policy. 'CUI Basic' requires no specific controls; 'CUI Specified' has particular handling controls, such as those required by the ITAR export regulations for example. CUI typically enables the government to carry out missions and business operations that affect the economy, security and national infrastructure of the U.S.

The Case For Compliance

While non-federal organizations will not be forced to comply with legislation to adopt the guidelines, they may be required to comply through the contracts they are issued by federal government, and the burden will be on them to meet the relevant legal and contractual obligations. Even if this is not the case, it will be in their own commercial interests to comply. Companies that can demonstrate the ability to apply the required controls on CUI will be more likely to win federal contracts.

Organizations that have never before had to protect CUI at this level will find themselves under pressure to comply with the final rule within the required timeframe, in order to remain qualified to compete. Fortunately, NIST permits non-federal organizations to protect CUI "using the systems and practices they already have in place, rather than trying to use government-specific approaches" – but for many there is still a hill to climb.

The Nuts And Bolts

The CUI framework is more about people than technology. At a basic level, it is geared towards ensuring that the right people have access to the data that relates to a particular contract, and that colleagues who are not working on the contract don't.

To comply, organizations will need to implement a comprehensive information security program. Even smaller, local companies must plan as though they are large, global enterprises – treating all points where data travels or resides as a location where CUI must be controlled.

They will be required to put in place a strong security plan with specific technical security and compliance documentation consistent with 14 security control families:

1. Access control
2. Awareness and training
3. Audit and accountability
4. Configuration management
5. Identification and authentication
6. Incident response
7. Maintenance
8. Media protection
9. Physical protection
10. Personnel security
11. Risk assessment
12. Security assessment
13. System and communications protection
14. System and information integrity

The framework's most critical element is the standardized labelling of CUI to ensure that appropriate protections can be implemented and consistently enforced. It is this labelling that makes the rule actionable in the daily working lives of those handling CUI.

The use of three CUI classifications is recommended, which should be clearly visible in the header and footer of relevant documents:

- **1. CUI Basic:** Subject to standard safeguarding measures that reduce the risks of unauthorized or inadvertent disclosure. Dissemination is permitted to the extent that it is reasonably believed that it would further the execution of a lawful or official purpose.
- **2. CUI Specified:** Requiring safeguarding measures that reduce the risk of unauthorized or inadvertent disclosure. The material should contain additional instructions on what dissemination is permitted.
- **3. Limited Dissemination:** Requiring safeguarding measures more stringent than normal, as the inadvertent or unauthorized disclosure would create risk of substantial harm. Again, the material will contain additional instructions.

The CUI Rule In A Nutshell:

- Defines the security requirements for protecting CUI in non-federal information systems and organizations
- Standardizes the handling of information that doesn't meet the criteria for classification under E.O. 13526, 'Classified National Security Information', or the Atomic Energy Act
- Specific guidance is the **National Institute of Standards and Technology (NIST) Special Publication 800-171**: Protecting Controlled Unclassified Information in Non-federal Information Systems and Organizations
- Driven by **Federal Acquisition Regulations (FAR) 52.204.17**, and the **Defense Department Federal Acquisition Regulations (DFARS) 252.204.2071** clauses

The markings should be used to alert individuals to the presence of CUI on documents, drawings, and emails – but also within downstream security controls that manage IT systems, devices, databases, USB sticks and CD ROMs.

Agencies and contractors that wish to work with the U.S. federal government need to be able to understand these markings on the CUI they come into contact with, and treat it in accordance with the classification policy. The challenge is that while NARA has set out the overlaying framework for labelling CUI, each government department and agency has been left to figure out its own control requirements.

Organizations can position themselves for compliance by taking steps to master the principles of data classification, and implement the tools and training that will enable them to accurately and consistently enforce a labelling policy.
By doing this they will be ready to show to federal government they have the capabilities in place to recognize and handle any type of marking, and also produce them where necessary.

The Principles Of Data Classification

It will normally be down to the originating agency or department to mark CUI, but partners and contractors need to understand how data classification works to treat it appropriately and operate in line with the policy set by the relevant federal organization.

Data classification involves the categorization and labelling of data. The approach places the focus of protection on the information itself, ensuring it is kept secure through its downstream journey.

- **A paper-based classification policy** - which sets out clearly how employees are required to treat the different types of data they handle.
- **Automated data classification** - where electronic markings are applied by software solutions that use key words or phrases in the content to analyze and classify it.
- **User-driven data classification** - - where the person producing or handling the data is responsible for deciding which label is appropriate, and attaching it at the point of creating, editing, sending or saving.

The 'gold standard' approach is one that involves both users and software toolsets to make control comprehensive.

The user's insight into the context, business value and sensitivity of a piece of CUI enables them to make informed and accurate decisions about the best label to apply. The integration of a data classification solution means that as well as the visual markings required by the CUI framework, the label will be embedded into the file properties as metadata. This then steers the actions of downstream enterprise security and data management solutions, allowing the CUI to be accessed or used only in accordance with the rules that correspond to its classification. A data loss prevention (DLP) solution, for example, can either block employees from uploading a file marked CUI to a Cloud file share service, or prevent it from being accessed by unauthorized individuals.

Another benefit to implementing a data classification solution is the detailed behavioral data generated through its monitoring and reporting function. This can be used to support the demonstration of compliance position – giving organizations the validation and evidence they need to demonstrate to regulators, the board, and clients' contracting officers that they are treating CUI correctly. It also highlights where users are not following policy, so this can be addressed through additional training.

Conclusion

Now we have concrete guidance around the treatment of CUI at last. We've got the regulation, and we've got the tools, so it is time to do the job.

Organizations that do not take steps to comply with the rule risk losing existing contracts or missing out on future opportunities. Failing to adequately protect CUI also has its implications – a data leak that exposes a client or breached regulation could lead to a damaged reputation and brand, penalties and the possible loss of business.

By choosing to adopt the framework, organizations will demonstrate the ability to protect federal government information, enhancing their ability to respond to new opportunities to work with the U.S. government.

The 5 Steps To Effective CUI Classification

1. Identify

Build a strong foundation of knowledge around the CUI you create, process, store and disseminate. Figure out what you need to do to comply with the new framework and with your contracting or partner organization's security policies. Understand the language they use, the types of information that need to be marked and what the markings mean.

2. Discover

Pinpoint exactly what CUI you are required to process, where it comes from, where it resides, where it is sent and who might have access to it. Once you have visibility of this establish what controls you need to put on it.

3. Classify

First, be clear on who should have access to each type of CUI. Select a technology solution that will enable users to consistently apply the classification scheme and will also add metadata. Start by classifying your 'live' data –the emails, files and documents that are being received, created and handled right now. Then move on to labelling the existing and legacy CUI that is stored and held around the organization.

4. Secure

Implement tools and solutions that will control and protect CUI through its journey. The metadata label will enable higher grade controls such as DLP solutions, security incident and event monitoring (SIEM) tools, access control tools and data governance tools to safeguard it when it's accessed or used later.

5. Monitor

The CUI framework is likely to evolve from its first iteration. Use monitoring and reporting tools to track how CUI is being accessed, used and classified in your organization, and provide the intelligence needed to evolve the approach in line with changes.

Global brands trust us to protect their sensitive data:

pwc

Ministry of Defence

Honeywell

PRUDENTIAL

DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA

AMGEN

SOCIETE GENERALE

Allianz

Raytheon

More Information

For more information about how you can implement a data classification solution as part of your data protection strategy, please **contact us**

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.