Deloitte.

5x5 series: Insights and actions

Safeguarding Controlled Unclassified Information (CUI)

CUI is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies. Given the increasing and persistent threats made by adversaries to obtain access to sensitive data (e.g., CUI), the need to protect such data has never been more important and federal government contractors are critical to this effort.

Protecting CUI is highly dependent on properly defining CUI in the context of your organization and scoping your CUI boundary accordingly – both of which can be extremely challenging. Many organizations struggle with these foundational efforts; however, the insights and actions below provide a helpful roadmap to safeguard CUI.

5 things you should know

- The **products and/or services** and the way in which your organization provides them to the federal government is not always clear.
- Understanding the National Archives and Records Administration (NARA) CUI guidance can help **in defining CUI data elements** relevant to your organization.
- The **NARA CUI guidance** should be applied to your organization's data governance program so that CUI data elements can be properly identified within your environment.
- **Alignment of tailored CUI definitions with your organization's federal business processes** (and supporting technologies) can enable your organization to identify its CUI footprint.
- Performing an **assessment of your organization's current state of compliance with relevant requirements** (e.g., NIST 800-171) can enable development of a clear roadmap for safeguarding CUI.

5 actions you can take

1. **Collaborate with relevant stakeholders across your organization** (e.g., IT, Procurement, Contracting, Legal) to understand how your organization engages with federal customers – including the product and/or services provided as well as possible CUI-relevant data elements.
2. Review publicly available CUI guidance and, if applicable, specific guidance provided to your organization by the government. **Develop a foundational understanding of what CUI is** and familiarize yourself with the various categories of CUI along with examples that are relevant to your organization.
3. **Define CUI in the context of your organization**. For example, which data elements relevant to your organization could be considered CUI.
4. Perform **CUI discovery exercises** to identify where CUI resides across your organization
5. Perform an assessment against the applicable requirements (e.g., 110 NIST 800-171 controls) to **identify compliance gaps and improvement opportunities**.

Click here to learn more about our CMMC services.

Connect with us:

ALAN FAVER
Partner | Deloitte & Touche LLP
afaver@deloitte.com

CHARAN AHLUWALIA
Principal | Deloitte & Touche LLP
cahluwalia@deloitte.com

KEITH THOMPSON
Managing Director | Deloitte & Touche LLP
keithompson@deloitte.com

MIKA ALEXOUDIS
Senior Manager | Deloitte & Touche LLP
malexoudis@deloitte.com