Controlled Unclassified Information—Will it Blindside the A/E/C Community?

The federal government is implementing changes to the cybersecurity requirements for handling data and information identified as sensitive and controlled.

By Anne C. Juran, P.E., LEED AP BD+C, CxA, M.SAME

Those working in the federal sector, specifically the Department of Defense (DOD) and General Services Administration (GSA), have seen contractor cybersecurity requirements taking shape since 2010. For Official Use Only and Sensitive But Unclassified, and their control policies, will be replaced by Controlled Unclassified Information (CUI) during 2017.

CUI is a program established by *Executive Order 13556* in November 2010 to manage "information that requires safeguarding or dissemination controls." The goal is to provide uniformity in labeling of these materials across the executive branch. The executive order established the National Archives and Records Administration as the manager of the program.

WHAT YOU MUST KNOW

As CUI rolls out during 2017, some of the requirements could be significant in time and cost, depending on how your firm's cyber systems are assembled.

In June 2015, National Institute of Standards and Technology (NIST) Special Publication 800-171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" was published. It identifies controls in Special Publication 800-53 that are applicable to federal contractors. This document was part of the defined pathway of items that needed to be completed prior to addressing CUI in the Federal Acquisition Regulation (FAR). It defines the minimum safeguarding requirements. Specified categories may have more requirements.

NIST Special Publication 800-171 is broken into 14 families, covering broad topics such as Access Control, Maintenance, Security Assessment, and System and Information Integrity. Examples of required controls include:

- *Audit and Accountability Family*, item 3.3.1: Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.
- *Incident Response Family*, item 3.6.1: Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.
- *Physical Protection Family*, item 3.10.2: Protect and monitor the physical facility and support infrastructure for those information systems.
- *Risk Assessment Family*, item 3.11.2: Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities are identified.

INCORPORATING INTO ACQUISITION

Most standard government contracts incorporate FAR clauses. On May 5, 2016, DOD, GSA, and the National Aeronautics and Space Administration incorporated basic safeguards into the FAR (48 CFR parts 4, 7, 12 and 52). Of special note, part 52 sets out safeguarding requirements for all systems that process, store, or transmit federal contract information, whether or not CUI. Part 52 also notes that additional requirements may be required for CUI.

On Sept. 14, 2016, Rule 32 CFR Part 2002 was published. It went into effect Nov. 14, 2016. The rule establishes CUI and the mandated cybersecurity controls. It sets requirements for executive agencies to implement the policy, including modifying terms of agreements that conflict with CUI.

An accompanying document, "CUI Notice 2016-01: Implementation Guidance for the Controlled Unclassified Information Program," dated Sept. 14, 2016, sets forth the implementation timeline. It gives agencies 180 days to implement new policies and modify or rescind all affected policies. Agencies have 180 days after the effective date of the agency policy to implement the policy and train all affected employees.

CUI: BASIC OR SPECIFIED?

CUI information can be labeled as basic or specified. Basic requires cybersecurity and other controls in accordance with NIST

Special Publication 800-171. A basic category has been established for DOD: Critical Infrastructure-DOD Critical Infrastructure Security Information (marked DCRIT). This basic category includes facilities in its description. Each "specified" category has additional controls that are identified in the CUI registry (www.archives.gov/cui/).

For federal government-focused members of the A/E/C community, three "specified" categories may be applicable: DOD's Controlled Technical Information (marked CTI); GSA's Critical Infrastructure, Physical Security (marked PHYS); and the Department of Homeland Security's Critical Infrastructure-Protected Critical Infrastructure Information (marked PCII). For DOD, it covers what is currently considered For Official Use Only. For GSA, it covers what is now Sensitive But Unclassified.

IMPLEMENTING CYBER CONTROLS

The Defense Federal Acquisition Regulation Supplement (DFARS) 48 CFR parts 202, 204, 239, and 252 252.204-7012 have undergone a number of changes regarding cybersecurity over the past three years. The final rule, dated Oct. 21, 2016, requires contractors and their subcontractors to protect Controlled Technical Information using the controls identified in NIST Special Publication 800-171.

While this requirement is not effective until Dec. 31, 2017, contractors are required within 30 days of contract award to identify those security controls that they have not implemented. This notification requirement is allowing DOD to monitor industry progress in implementing the controls.

THE FUTURE OUTLOOK

With the final rule for 32 CFR 2002 having been issued and CUI requirements incorporated into the FAR and DFARS, agency-specific guidance, such as DoDM 5200.01, Navy FC 1-300-09N, and GSA PBS P-100, should be updated by November 2017. 32 CFR 2002 specifies that all agencies must comply with CUI.

While waivers can be granted to support legacy markings, such as For Official Use Only, those markings must be switched to CUI if the material is disseminated outside of the designating agency.

However, there are also some understandable liberties taken with the requirements, including 2002.20(a)(8):

"When it is impractical for an agency to individually mark CUI due to quantity or nature of the information, or when an agency has issued a limited CUI marking waiver, authorized holders must make recipients aware of the information's CUI status using an alternate marking method that is readily apparent (for example, through user access agreements, a computer system digital splash screen (e.g., alerts that flash up when accessing the system), or signs in storage areas or on containers)."

If you have been in a client's Drawing Vault, you can see where the "signs in storage areas" component could complicate A/E/C work. Existing building documentation for an entire base could now be labeled as CUI just by putting a sign on the door. As a community, we must be vigilant about establishing CUI requirements in the fee proposal and contract stages and in making sure all material provided to us is consistent with the markings designated in the contract. We also have to be careful not to accept information with legacy markings.

Don't let your firm be blindsided!

TME

Anne C. Juran, P.E., LEED AP BD+C, CxA, M.SAME, is Senior Mechanical Engineer, Summer Consultants Inc.; 703-556-8820, or juran@summerconsultants.com.

As a community, we must be vigilant about establishing CUI requirements in the fee proposal and contract stages and in making sure all material provided to us is consistent with the markings designated in the contract.

HOW TO AVOID GETTING BLINDSIDED

- Make sure your fee proposals and contracts clearly designate any CUI requirements and make sure your subcontracts include the same requirements.
- Make sure any information that you are provided is consistent with the CUI requirements, or lack thereof, identified in your contract.
- Do not accept information (such as CDs) with markings that differ from your contract or that use legacy markings
- Watch for adjustments over the next year to agency procedures, such as DoDM 5200.01, Navy FC 1-300-09N, and GSA PBS P-100.
- Evaluate your systems/facility for compliance with the CUI Basic controls that are identified in NIST Special Publication 800-171.
- Educate your staff on the upcoming changes.
- Look for how changes to the FAR and DFARS will be received throughout 2017.