What Small Businesses Need to Know: Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

Department of the Navy Chief Information Officer

Background:

On November 4, 2010, the President signed Executive Order 13556, *Controlled Unclassified* Information (CUI). The Executive Order established a governmentwide CUI Program to standardize the way the executive branch handles unclassified information that requires protection. It designated the National Archives and Records Administration (NARA) as the Executive Agent to implement the program. The Executive Order 13556 also required that the CUI Program emphasize openness, transparency, and uniformity of governmentwide practices.

What is the purpose of NIST SP 800-171?

The purpose of this publication is to provide federal agencies with requirements for protecting the confidentiality of CUI:

- When the CUI is resident in nonfederal information systems and organizations.
- Where the CUI does not have specific safeguarding requirements prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category or subcategory listed in the CUI Registry.
- When the information systems where the CUI resides are not operated by organizations on behalf of the federal government.

What is adequate security?

The set of minimum cybersecurity standards are described in NIST SP 800-171 and break down into 14 areas or "Families."

FAMILY	FAMILY
Access Control	Media Protection
Awareness and Training	Personnel Security
Audit and Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification and Authentication	Security Assessment
Incident Response	System and Communications Protection
Maintenance	System and Information Integrity

Security Requirements (14 Families):
Obtained from FIPS 200 and NIST SP 800-53

In each of these areas, there are specific security requirements that contractors must implement at contract award. Prior to contract award, the contractor may propose alternate, equally effective, measures to DoD CIO. Within 30 days of contract award, the contractor must notify DoD CIO (osd.dibcsia@mail.mil) of any of the security requirements specified by NIST SP 800-171 that are not implemented at contract award. Full compliance is required no later than December 31, 2017.

If it is determined that other measures are required to provide adequate security in a dynamic environment based on an assessed or emergent risk or vulnerability, contractors may also be required to implement additional security precautions.

May contractors outsource these requirements?

Contractors may use subcontractors and/or outsource information technology requirements, but they are responsible for ensuring that these entities meet the cybersecurity standards.

Resources:

DoD's Office of Small Business Programs has put together a comprehensive list of cybersecurity resources for small businesses on its website:

http://business.defense.gov/Resources.aspx

The DON also has an Office of Small Business Programs (OSBP) that is dedicated to assisting small businesses. Visit OSBP's website at: http://www.secnav.navy.mil/smallbusiness/pages/index.aspx or contact OSBP at OSBP.info@navy.mil.

Sources:

NIST Special Publication 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations: *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf*

Federal Information Processing Standards Publication (FIPS PUB 200), "Minimum Security Requirements for Federal Information and Information Systems: *http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf*

NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations: *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf*

Defense Federal Acquisition Regulation Supplement, 252.204-7008 Compliance with Safeguarding Covered Defense Information Controls and 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting: *https://www.gpo.gov/fdsys/pkg/FR-2015-12-30/pdf/2015-32869.pdf*

Defense Cybersecurity Requirements: What Small Businesses Need to Know, Office of Small Business Programs, U.S. Department of Defense *http://www.acq.osd.mil/osbp/docs/Cybersecurity_04272016.pdf*