Question and Answer Summary for the NIST Small Business Cybersecurity Webinar — *Protecting Controlled Unclassified Information: Overview of the NIST Special Publication 800-171, Revision 3 Small Business Primer*

Overview

On January 20, 2026, NIST held the webinar "NIST Small Business Cybersecurity Webinar — Protecting Controlled Unclassified Information: Overview of the NIST Special Publication 800-171, Revision 3 Small Business Primer." View the event recording and slides here.

Event Speakers:

- Victoria Pillitteri, Co-Author of NIST SP 800-171, NIST
- Daniel Eliot, Lead for Small Business Engagement, NIST

The speakers welcomed questions from the audience during the webinar. Below is a summary of audience questions and associated responses. In most cases, the questions are written verbatim as submitted to NIST. Some questions have been slightly rephrased in order to combine multiple questions on the same topic.

Question	Answer
There were multiple questions about the Department of Defense (DOD) Cybersecurity Maturity Model Certification (CMMC) Program, including recommendations for vendors and how to get certified.	NIST cannot speak on behalf of the CMMC Program. For more information about the CMMC, including additional resources, see https://dodcio.defense.gov/CMMC/.
There were multiple implementation-specific questions.	NIST does not generally comment on or evaluate the implementation of requirements or "compliance." If there are additional questions about NIST's Protecting Controlled Unclassified Information (CUI) series, email sec-cert@nist.gov.
There were multiple questions about which revision of SP 800-171/SP 800-171A to use.	The CMMC Program currently leverages the requirements and assessment procedures in SP 800-171r2 (Revision 2) and SP 800-171A. Organizations can leverage the NIST-created change analysis (SP 800-171r2 to r3) to determine which revision best meets their current and future needs.
What types of small businesses (in which industries) need to meet SP 800-171 requirements? What is the relevance of SP 800-171 to small businesses?	Currently, the defense industrial base is the largest user community of NIST's Protecting CUI series through the Defense Federal Acquisition Regulation Supplement (DFARS) and CMMC requirements. Even if your organization does not have a contract that requires implementation of the SP 800-171 security requirements, you can still elect to use the requirements to protect the confidentiality of any information, even if it is not CUI. Like all NIST cybersecurity and privacy guidelines, the Protecting CUI series

	(i.e., SP 800-171, SP 800-171A, SP 800-172, and SP 800-172A) does not provide "regulatory guidance." These guidelines are designed for and scoped to protecting controlled unclassified information.
If an organization is SOC-2 or SOC-3 compliant, is it automatically compliant with SP 800-171 security requirements?	NIST does not determine reciprocity of the SP 800-171 security requirements with other standards. Rather, the agency that mandates use of the SP 800-171 security requirements determines any acceptable alternatives. A useful NIST resource is the Online Informative References Tool, which helps subject-matter experts define standardized online informative references (OLIRs) between elements of their documents, products, and services and elements of NIST documents. *Note that only some OLIRs are developed by NIST; others are developed and submitted by other organizations and are not reviewed by NIST for technical accuracy*.
Could there be a variation in control implementation, depending on the size of the business? One that would incur lesser costs than non-smalls? How many FTEs are needed to implement?	Implementation of the SP 800-171 security requirements will vary from organization to organization, as would the resources needed (e.g., staffing, funding). Factors that impact implementation could include scope (i.e., how the system or subsystem is scoped), use of custom-solutions, or a third-party solution or service.
Why only confidentiality- and not integrity- and availability-focused?	As defined in 32 CFR § 2002.14, CUI should be protected at no less than the moderate confidentiality impact level. As such, the scope of SP 800-171 is tailored from the SP 800-53B moderate impact level to focus on confidentiality. *Note that the enhanced security requirements in SP 800-172 address confidentiality, integrity, and availability.*
How is CUI implemented for a business that needs to get off the ground and be secure/compliant?	It is the responsibility of the federal agency or prime contractor you are working with to identify relevant requirements in contracts or other agreements and for the federal agency to identify and mark CUI. The agency that is imposing the requirements determines whether your implementation is "compliant." *Note that "compliant" and "secure" are not necessarily synonymous.*
Who is responsible for defining ODPs?	The determination of ODP values can be guided and informed by laws, Executive Orders, directives, regulations, policies, standards, guidance, or mission and business needs. If a federal agency or consortium of agencies do not specify a particular value or range of values for an ODP, nonfederal organizations must assign those values to complete the security requirement.
What is NIST['s] definition of small business? Based on size?	NIST uses the U.S. Small Business Administration's small business size standards.

Is there a [small business] primer for SP 800-171, Revision 2?	There is not a small business primer for SP 800-171r2. However, the small business primer for Revision 3 outlines key differences between Revisions 2 and 3.
Does NIST provide a list of recommended vendors to assist with implementation and assessment?	NIST does not endorse specific products or services. You may explore the CyberAB Marketplace* or MSPs for the Protection of Critical Infrastructure* to find and evaluate consulting firms who may assist in SP 800-171 implementation. **Note that non-NIST sites are included because they may have information of interest to readers. NIST does not necessarily endorse the views expressed or the facts presented on those sites. Further, NIST does not endorse any commercial products that may be advertised or available on these sites.*
Are there case studies on small businesses that have implemented SP 800-171?	NIST does not currently have case studies on small businesses that have implemented SP 800-171, but if organizations are interested in working with NIST on this, please submit inquiries to smallbizsecurity@nist.gov.
Is there a spreadsheet containing all the SP 800-171A, Revision 3 assessment objectives?	You can export data from the Cybersecurity and Privacy Reference Tool.
Is SP 800-171, Revision 3 available to download in PDF format?	Yes, you can download it as a PDF or you can view it interactively via the Cybersecurity and Privacy Reference Tool and export it into JSON or Excel.
Is there a crosswalk between SP 800-171 and CSF?	You can view a crosswalk between the functions and categories in Cybersecurity Framework (CSF) 2.0 and the SP 800-171r3 CUI requirements in the National Online Informative References (OLIR) Program database.
For small businesses, does NIST recommend SP 800-171 over CSF, CIS Controls, etc.?	The NIST cybersecurity control sets (e.g., SP 800-53, SP 800-171) serve distinct but complementary purposes from the CSF and can be used together. For small businesses, you might consider starting with the CSF 2.0 Small Business Quick-Start Guide.

Key Resources

Resource	Description
SP 800-171r3 *Protecting Controlled Unclassified Information in Nonfederal Systems*	SP 800-171r3 is a set of recommended security requirements for protecting the confidentiality of CUI.
SP 800-171Ar3 *Assessing Security Requirements for Controlled Unclassified Information*	SP 800-171Ar3 provides assessment procedures and a methodology to conduct assessments of the CUI security requirements in SP 800-171.
SP 800-171r3 Small Business Primer	This guide provides small businesses with an overview of SP 800-171r3.
SP 800-171r3 FAQ	These frequently asked questions (FAQ) provide background information and rationale for the changes in SP 800-171r3 and SP 800-171Ar3.
Cybersecurity and Privacy Reference Tool (CPRT)	CPRT provides online, interactive versions of the updated security requirements in SP 800-171r3 and the updated assessment procedures in SP 800-171Ar3.
SP 800-18r1 *Guide for Developing Security Plans for Federal Information Systems*	SP 800-18r1 introduces a set of activities and concepts for developing an information system security plan.
SP 800-161r1 *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*	SP 800-161r1 provides guidelines on identifying, assessing, and mitigating cybersecurity risks throughout the supply chain at all levels of an organization.
SP 800-30r1 *Guide for Conducting Risk Assessments*	SP 800-30r1 provides guidelines for conducting risk assessments of federal information systems and organizations.
NIST Small Business Cybersecurity Corner	This website is the hub for NIST's small business cybersecurity activity and resources.
NIST Small Business Cybersecurity Corner's Government Contractor Resources	This website lists resources from the Federal Government and non-profits to help small businesses address the cybersecurity requirements of federal customers.
NIST Small Business Cybersecurity Community of Interest	NIST's Small Business Cybersecurity Community of Interest (COI) allows the public and private sectors to share business insights, expertise, challenges, and perspectives to help NIST address the cybersecurity needs of the small businesses community.
NIST Computer Security Resource Center **(CSRC)**	The NIST Cybersecurity and Privacy Program develops and maintains an extensive collection of standards, guidelines, recommendations, and research on the security and privacy of information and information systems.
Sign up for updates from NIST	Subscribe to one or many lists to receive updates on topics you care about the most.