PREVEIL

Getting Started with NIST SP 800-171 Compliance in Higher Education

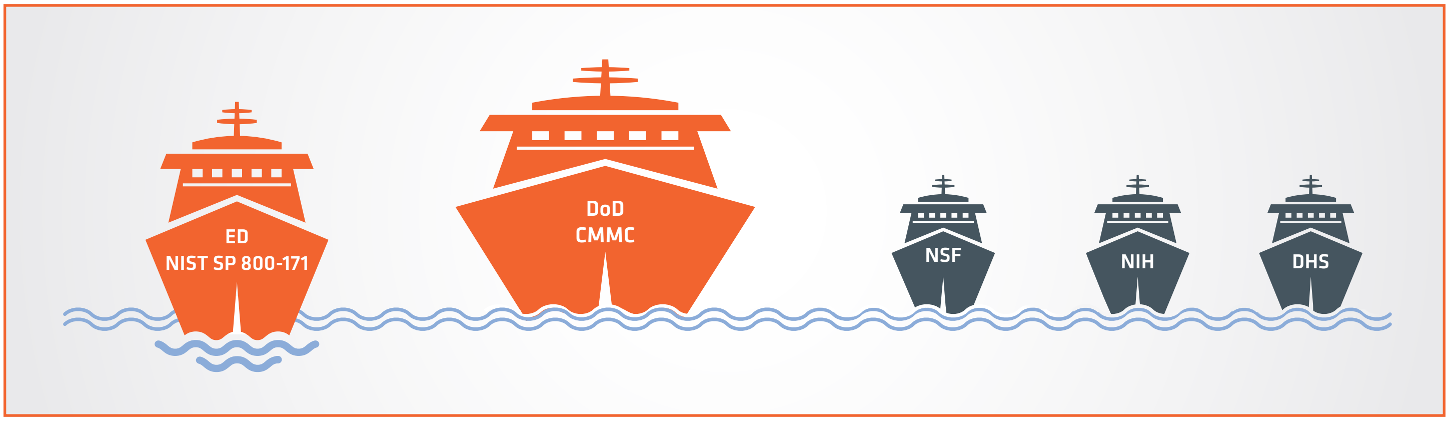
What is NIST SP 800-171?

The National Institute of Standards and Technology (NIST) Special Publication 800-171, *Protecting Controlled Unclassified Information [CUI] in Non-Federal Information Systems and Organizations*, defines the security requirements, or controls, required to protect CUI that's shared by the federal government with non-federal information systems and organizations. The aim of the NIST special publication is to standardize how the federal government handles unclassified information that requires protection.

(Non)Enforcement

NIST SP 800-171 was released in mid-2015. The Department of Defense (DoD) moved quickly to incorporate the NIST security controls into its contracts: by late 2016, DFARS clause 252.204.7012 required all organizations that do work for the DoD and handle CUI to assess and document their compliance with NIST SP 800-171 security standards. This includes defense work done by university-based research labs and facilities, as well as FFRDCs (Federally Funded Research and Development Centers) and UARCs (University Affiliated Research Centers).

Other federal agencies, however, continued to rely largely on pre-existing laws or regulations rather than develop contractual FAR (Federal Acquisition Regulation) clauses like the DoD's related to NIST SP 800-171. The Department of Education (ED), for example, historically has relied on the SAIG Enrollment Agreement and the Gramm-Leach-Bliley Act (GLBA) Safeguard Rule, among others, to obligate colleges and universities to safeguard ED-related CUI. Indeed, a Dear Colleague letter issued in July 2016 by the ED simply "reminded" institutions of their legal obligations to protect student information used in the administration of the Title IV Federal student financial aid programs.

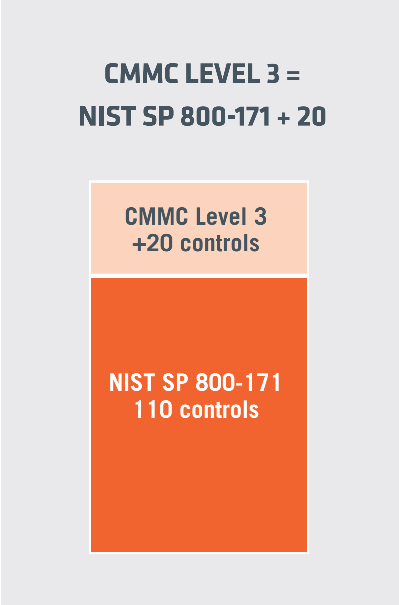


Why NIST SP 800-171 matters now: Enforcement

Not even the DoD has been enforcing NIST SP 800-171 requirements. Prior to 2021, companies in the Defense Industrial Base (DIB) only had to conduct self-assessments and self-attest to their compliance with the NIST SP 800-171 security controls. That's changing.

As of late 2020, the DoD is requiring that NIST SP 800-171 self-assessments be conducted according to a carefully defined DoD Assessment Methodology, and self-assessment scores have to be filed with the DoD's SPRS (Supplier Performance Risk System). Scores less than a perfect 110 necessitate the creation of a POAM (Plan of Action and Milestones) and an indication to the DoD as to when security gaps will be remediated.

Further, DoD has begun to roll out its new Cybersecurity Maturity Model Certification (CMMC) framework, which measures an organization's ability to protect FCI (Federal Contract Information) and CUI. CMMC has five defined levels of cybersecurity maturity; Level 3 is built on NIST 800-171's 110 controls, plus an additional 20 controls. PreVeil and EDUCAUSE collaborated on a white paper, *Higher Education, Research, Cybersecurity, and CMMC Compliance*, to help guide institutions on their journey to CMMC compliance.


CMMC LEVEL 3 =
NIST SP 800-171 + 20

Department of Education and other federal agencies following DoD's lead

The Department of Education's Federal Student Aid Office (FSA) is following the DoD's lead in implementing and enforcing higher cybersecurity standards. FSA has created a Campus Cybersecurity Program, and in December 2020 issued an announcement, *Protecting Student Information: Compliance with CUI and GLBA*, to "inform IHEs [Institutions of Higher Education] and their third-party servicers about upcoming activities to ensure compliance with NIST 800-171 Rev. 2." Those activities have begun.

> "FSA's notice makes one thing clear, even if it leaves many other issues unresolved: FSA intends to begin moving *this year* toward requiring institutional compliance with the NIST 800-171 guidelines in relation to the FSA data that institutions receive… Colleges and universities that have not yet started down the road to implementing 800-171 may not have the luxury of waiting much longer to begin. "
>
> –JARRET CUMMINGS
> EDUCAUSE SENIOR
> ADVISOR FOR POLICY AND
> GOVERNMENT RELATIONS

The Department of Education recently stated that it considers most data sourced from the Department and information used in the administration of Title IV programs to be CUI.

FSA's December 2020 announcement makes clear that implementation of NIST 800-171 controls will form the foundation of its Campus Cybersecurity Program. FSA describes a "multi-year phased implementation" of NIST 800-171 controls, beginning with a self-assessment of the IHE community's "readiness to comply." ED's aim is to "determine the cybersecurity posture, maturity, and future compliance of each IHE with NIST 800-171 and other cybersecurity requirements."

Federal agencies most relevant to HEIs ramping up cybersecurity requirements

EDUCAUSE and other higher education organizations are working with FSA to address the numerous issues and questions raised by the FSA announcement to enforce NIST 800-171.

The DoD and ED are not alone is ramping up cybersecurity requirements: other federal organizations moving in the same direction include DHS, NIH and NSF. In fact, the US General Services Administration (GSA) released an RFP back in July 2020 that required compliance with the DoD's CMMC program, noting that noncompliance with CMMC would disqualify bidders.

Steps to take now to comply with NIST SP 800-171

Taking action now to improve your institution's cybersecurity posture will help you protect student data and the systems you use to collect, process and distribute that information, including PII. Your institution's enhanced security practices also will help you achieve compliance with NIST SP 800-171 and allow you to continue to do your work without interruption brought on by cyberthieves, hackers, and other bad actors.

LEARN MORE

- Review FSA's Dec. 2020 announcement, *Protecting Student Information: Compliance with CUI and GLBA*, and see EDUCAUSE's early policy analysis of the announcement, *800-171 Compliance on the Horizon*.
- Familiarize yourself with NIST SP 800-171 requirements. EDUCAUSE's paper, *An Introduction to NIST Special Publication 800-171 for Higher Education Institutions* is a good place to start.
- Evaluate your current security posture in relation to NIST SP 800-171 to identify gaps. BYU's Office of Computing Research has created a helpful NIST SP 800-171 Assessment Tool. Or you may wish to conduct a self-assessment based on the DoD's NIST SP 800-171 Assessment Methodology.

CONSIDER PREVEIL'S STATE-OF-THE-ART TECHNOLOGY SOLUTION TO CLOSE YOUR CYBERSECURITY GAPS

PreVeil is an email and file sharing platform that provides **uncompromised security for protecting and exchanging CUI.** It's grounded in a modern Zero Trust environment and end-to-end encryption. All user data is only ever encrypted and decrypted on a user's device—and never on a server.

PreVeil Drive offers **data visibility and access control,** so that files can be shared with different permissions and expirations, allowing the highest levels of control over CUI. Admins can view activity logs and decrypt and export user data—provided they have permission from a pre-determined Approval Group.

PreVeil's solutions support **compliance with NIST SP 800-171, as well as with DFARS 252.204-7012, and CMMC Level 3**. PreVeil is FedRAMP Baseline Moderate Equivalent and stores all data on Amazon Web Services GovCloud, which is FedRAMP High.

PreVeil Email and Drive deploy easily as an overlay system, with no impact on existing file and email servers, **making deployment and configuration simple and inexpensive.** Deployment can be completed in a matter of hours.

PreVeil is **easy for users to adopt** because it works with the tools they already use: PreVeil Drive's file sharing works like OneDrive and is integrated with Windows File Explorer and Mac Finder. PreVeil Email seamlessly integrates with Outlook, Gmail, or Apple Mail clients. Users can keep their regular email address.

Given its ease of deployment and use, PreVeil is **cost effective.** It needs to be deployed only for employees that handle CUI, whereas alternatives require deployment across entire organizations.

CASE STUDY: NIST 800-171 COMPLIANCE

DIBCAC (the Defense Industrial Base Cybersecurity Assessment Center) recently conducted a thorough audit of a small defense subcontractor using DoD's exhaustive Assessment Methodology. The subcontractor, which uses 0365, was able to keep that system and simply overlay PreVeil in a matter of hours to help address the majority of NIST 800-171 controls. The SMB achieved a remarkably near-perfect score on the audit, and clearly is well on its way toward CMMC Level 3 compliance.

PREVEIL

For more information on NIST SP 800-171 compliance in higher education, contact:

BRIAN KELLY
Cybersecurity Program Director, EDUCAUSE
1150 18th Street, NW
Washington, DC 20036
(202) 872-4200
bkelly@educause.edu
@BKinCT

SANJEEV VERMA
Chairman, PreVeil
85 Devonshire Street, 8th Floor
Boston, MA. 02109
(857) 353-6480
sanjeev@preveil.com
www.linkedin.com/in/Sanjeev-Verma-PreVeil

April 2021