# NIST 800-171: FAQs

1. **What is NIST 800-171?**

   NIST 800-171 is the publication the National Institute of Standards and Technology (NIST) that set forth standards and controls to protect Controlled Unclassified Information (CUI) used in non-federal systems and institutions such as a UC campus.

2. **What is Controlled Unclassified Information?**

   CUI is an information classification used by the federal government. There are two distinct categories of information generated by the federal government, “classified” and “unclassified”. Within the unclassified category, individual federal agencies determine categories of information that require additional protection against disclosure and unauthorized access. In order to harmonize these sub categories of unclassified information, Executive Order 13556 was published in 2010 instituting the CUI category. The type of information that is considered CUI can be found at Controlled Unclassified Information Registry. Only federal agencies determine what is CUI and what is not.

3. **What are the security requirements necessary to comply with NIST 800-171?**

   There are numerous requirements that must be met in order to comply with the NIST 800-171 standards. Security requirements include controls in a variety of areas, including access controls, training, systems management, identification and authorization, physical security, risk assessment and numerous other information security area. These requirements are complex, and are not part of security requirements you would normally find in academic research and computing.

4. **How does NIST 800-171 apply to UC Merced?**

   NIST 800-171 will apply to all academic research institutions that receive, have, use, and/or store CUI in connection with a variety of transactions with the federal government. Examples of CUI that higher education institutions might receive from a federal agency include:

   - Student records or personally identifiable information (PII)
   - Student financial aid data
   - Research data
   - Controlled technical information
   - Critical infrastructure information.

   NIST 800-171 requirements may be included as a part of the terms and conditions of government documents, most commonly in contracts with the federal government, but also in research grants and awards, data use and/or sharing agreements, patent application agreements, and a variety of other documented transactions between the federal government and academic research institutions.

5. **When do we have to comply with these requirements?**

   Currently only the Depart of Defense (DoD) requires compliance with NIST 800-171 standards in their contracts; DoD compliance is required effective December 31, 2017. However, the Department of Education (DOE) is encouraging compliance in grants and contracts where CUI is received by the academic research institution (Please see Dear Colleague Letter). It is important for all institutions to survey any federal contracts, but especially DoD  contracts, to which it may be a party to determine if the NIST 800-171 standards are required.

6. **How do I know when NIST 800-171 applies?**

   If NIST 800 171 applies, the contract with the federal agency will designate the information received as CUI, and the contract will specify 1) the data specifically identified as CUI received from the federal government, and 2) that the institution must follow the terms of NIST 800-171. In some cases the contract may reference DFARS clause 252.204-7012. In these cases, the same requirements apply.

7. **What do I do when a federal contract requires NIST 800-171 be followed?**

   Contact the UC Merced Office of Information Technology immediately upon determining NIST 800-171 compliance is required. The security standards are complex and can take substantial time to put into place. Please contact: Chief Information Security Officer Nick Dugan at ndugan@ucmerced.edu

8. **What happens if we cannot or do not comply with NIST 800-171 when required to do so?**

   If the University finds it cannot comply with NIST 800-171 in contract or grant, it is likely that we cannot accept the contract or grant. If we do not comply with the requirement, we risk a variety of penalties from the federal government, including substantial fines.

9. **Where can I read more about NIST 800-171?**
   - An Introduction to NIST Special Publication 800-171 for Higher Education Institutions
   - Department of Education Dear Colleague Letter
   - Presentation by Government Accountability Office (GAO)
   - The EDUCAUSE NIST 800-171 Resource Page

10. **Who do I contact when I have questions? You may contact either CISO Nick Dugan (ndugan@ucmerced.edu) or AVC Deborah Motton (dmotton@ucmerced.edu).**