FAR CUI Compliance for Universities and Research Institutions

Earlier this year, the Federal Acquisition Regulation (FAR) Council proposed a new rule in an effort to standardize how federal agencies and contractors handle CUI (controlled unclassified information). The purpose of this rule is to establish uniform guidelines for handling and securing CUI in order to safeguard sensitive government data handled on both federal and non-federal information systems. This is critical, as the absence of standardized guidelines for handling CUI has created a complex network of regulations across federal departments and agencies that can create confusion for contractors and lead to security gaps. The new rule will consolidate these requirements and provide a new cybersecurity standard for all organizations handling CUI by requiring them to maintain compliance with the security controls outlined in NIST SP 800-171.

Yet, considering the growing role universities and research institutions play in government-funded projects, you may find yourself wondering whether your educational institution must comply with the FAR CUI Proposed Rule. The short answer is that any institution, educational or otherwise, that handles CUI on behalf of the federal government must comply with FAR CUI. Keep reading to learn more about how the proposed FAR CUI rule will affect educational institutions, and how you will know if your institution is affected.

When Do Educational Institutions Need to Follow FAR CUI Compliance?

The biggest question you may have is how you will know whether FAR CUI applies to your university. Determining whether or not your institution must maintain FAR CUI compliance is essential, as failing to do so could result in serious penalties and legal action (more on this later). While this is not a complete list of when an educational institution needs to comply with FAR CUI, a few common examples include:

- **Universities Receiving Federal Grants or Contracts Involving CUI:** If your university does contract work for the federal government, or you receive federal grants, and as a result, you handle CUI, then the FAR CUI rule would apply to your organization.
- **Research Institutions Partnering With Government Agencies:** If you have a partnership with a government agency such as the Department of Defense (DoD), NASA, or NSF that requires you to handle CUI, you would be subject to FAR CUI.
- **Collaborations with Federal Contractors:** Even if you do not have direct contracts with a government agency, if you work with federal contractors and handle CUI as a result, you would also be subject to FAR CUI.
- **You Handle CUI for Any Reason:** If your institution handles CUI for any reason, then you would need to maintain FAR CUI compliance.

Compliance Requirements for Educational Institutions

If you determine that your university must comply with FAR CUI once this rule goes into effect, you may find yourself wondering what your compliance obligations will include. Educational institutions will face a variety of compliance requirements, including:

- **Implementing NIST SP 800-171 Security Controls:** In order to achieve compliance with FAR CUI, affected universities will have to achieve compliance with all 97 security controls outlined in NIST SP 800-171. This process will include implementing access controls, encryption, and data monitoring to ensure the proper protection of CUI handled by your institution.
- **Cybersecurity Measures for CUI Protection:** To achieve compliance with the security controls outlined in NIST SP 800-171, you will also have to implement robust cybersecurity measures to ensure the proper protection of CUI. This includes ensuring federally funded research data is stored securely, as well as implementing strong identity and access management (IAM) policies to prevent CUI from being accessed by unauthorized personnel.
- **Training and Awareness for Faculty and Researchers:** All individuals with access to CUI, including faculty, staff, researchers, and student researchers, will need to undergo regular training on the proper identification, management, and handling of CUI. This should also include regular security awareness training to ensure that your team stays up-to-date on cybersecurity best practices.
- **Incident Reporting and Risk Management:** To ensure compliance with FAR CUI, you must also maintain strict incident reporting procedures, as universities must report security incidents involving CUI within 8 hours. Of course, the best course of action would be to prevent such a breach, which is why it's essential that you have robust risk management procedures in place.

Challenges in FAR CUI Compliance for Universities

While achieving compliance with FAR CUI is essential for educational institutions with government contracts to protect sensitive data, this is no simple feat. The fact is that universities may face a variety of challenges and roadblocks as they attempt to navigate the compliance process. One of the biggest challenges these institutions will face is in trying to balance academic freedom with federal security controls. The restrictions imposed by FAR CUI can reduce academic freedom by limiting how they share research data with their faculty, students, and their academic research partners. Additionally, the need to implement robust security measures and training protocols across multiple departments and projects can also be

a significant burden that can be a drain on an institution's already limited resources. For many universities, insufficient funding and a lack of dedicated staff can be major barriers to FAR CUI compliance.

Steps Educational Institutions Can Take to Ensure Compliance

Given the challenging nature of complying with FAR CUI, educational institutions may find themselves unsure where to start their compliance journey. To help get you started, here are a few steps that you can take to help ensure compliance with FAR CUI.

- **Identify CUI:** Before you can start creating a plan to achieve compliance with FAR CUI, you must first identify where CUI exists within your university's systems. This will involve reviewing your government contracts and federally funded projects to identify the CUI that your institution handles.
- **Conduct a Gap Assessment:** Next, you should evaluate your organization's existing cybersecurity posture against the security controls outlined in NIST SP 800-171 to identify gaps in your compliance posture. You can then develop a roadmap to address these gaps and achieve compliance with FAR CUI.
- **Implement Secure Cloud Storage Solutions:** If your institution operates in a cloud environment, or you plan on migrating to the cloud soon, it's essential that you choose a secure cloud storage solution that is compliant with NIST SP 800-171, such as Microsoft GCC. The fact is that the wrong cloud solution could put the CUI you handle (as well as your sensitive research) at risk.
- **Train Everyone Handling CUI:** Even if you have robust security measures in place to protect CUI, your data could still be vulnerable if those who handle it don't take the proper precautions. This makes it essential that you ensure everyone who handles CUI, including faculty, students, and researchers, receives comprehensive training on how to identify, handle, and protect the CUI they interact with. Training should be ongoing to ensure everyone is up to date on the latest practices for protecting CUI.
- **Develop CUI Monitoring Policies:** You should also take the time to develop and implement policies for monitoring CUI, including those that help you detect and address gaps in your compliance posture.

What Happens if Universities Don't Comply?

As we previously mentioned, universities face numerous challenges and obstacles when attempting to achieve compliance with FAR CUI. However, educational institutions that handle CUI must make achieving compliance a priority, as non-compliance can result in serious

repercussions, including:

- **Loss of Federal Funding:** If an affected university is found out of compliance with FAR CUI, this can result in the suspension or termination of government contracts. These institutions may also be ineligible for future government contracts or research awards, and they may also lose their current research funding. Failure to comply with FAR CUI can then have devastating consequences by jeopardizing substantial government funding.
- **Legal Repercussions:** Not only may non-compliant universities lose their government contracts, but they may even find themselves facing financial and legal repercussions. These institutions may be fined for not adhering to FAR requirements, and they may also be financially liable for government costs incurred when responding to and mitigating CUI incidents resulting from the institution's negligence. Additionally, these universities may also face legal action for breach of contract.
- **Reputational Damage:** Failure to comply with FAR CUI can also cause universities serious reputational harm, which can affect their ability to attract future contracts and partnerships.
- **Potential Cybersecurity Vulnerabilities:** Not only does failure to comply with FAR CUI put universities in breach of their government contracts, but it can also put them at risk of a costly cyberattack. Without the proper cybersecurity measures in place, universities become an easy target for malicious agents looking to access sensitive research data.

For educational Institutions that handle CUI, achieving compliance with the new FAR CUI rule is essential. Not only will this ensure that you've met your contractual obligations so that you do not face any fines or legal repercussions, but it's also critical in ensuring that the sensitive research data you handle does not fall into the wrong hands. In order to properly protect the sensitive government data you handle, your institution then needs to implement proactive security measures, including robust cybersecurity, identity and access management, and data monitoring policies. Yet, complying with FAR CUI can feel like an overwhelming prospect, and you may be unsure where to start. The good news is that you do not need to face compliance alone. If you need help ensuring FAR CUI compliance for your institution, contact [redacted] today to learn about our cybersecurity services.