

More IT compliance requirements headed your way (NIST 800-171 CUI Security)



ARTICLE 03.18.21 DEAN DORTON

This past December, Federal Student Aid – US Department of Education posted a letter addressing Compliance with CUI and GLBA. CUI stands for Controlled Unclassified Information, and the letter lays out cybersecurity requirements related to CUI. The questions you may be asking are:

- [What makes data CUI?](#)
- [What are the new cybersecurity requirements?](#)
- [Is this the same as GLBA compliance?](#)
 - [Is this replacing or in addition to GLBA compliance?](#)
 - [Will there be audits and compliance testing for both GLBA and the new cybersecurity requirements?](#)
- [When will this impact my institution?](#)
- [How much more compliance overhead is this going to create?](#)

The December letter has the latest guidance available. Some of the answers to the questions are provided, some are hiding between the lines, and others require an educated guess.

What Makes Data CUI?

Let's start off with the easiest question. CUI is anything designated by a federal agency as "CUI" or "Controlled". If it is not designated, it is not CUI. That the FSA letter was issued means FSA considers student financial aid data as CUI.

What is NIST 800-171?

The new cybersecurity requirements are NIST 800-171r2. NIST 800-171r2 is a cybersecurity framework that has been adopted in whole by FSA as a set of compliance requirements. They encompass 109 controls that have been mapped to other cybersecurity frameworks, such as ISO, as well as compliance requirements, such as HIPAA.

Is this the same as GLBA compliance? Is this replacing or in addition to GLBA compliance?

Next, we can address all the GLBA questions together. From a compliance standpoint, the new cybersecurity requirements appear to be additive to the GLBA requirements. In other words, institutions of higher education (IHE) will need to comply with both. Fortunately, the silver lining is the amount of overlap between the two. Complying with the new cybersecurity requirements will satisfy all but one of the GLBA requirements.

All IHEs should be compliant by now with FSA GLBA requirements if they are providing financial aid to students. Therefore, all GLBA compliance efforts were worthwhile and not a waste of time. To put it into perspective, if you have performed a GLBA risk assessment and did not use the NIST framework your compliance efforts and overlap with the new cybersecurity requirements resemble the diagram below. If you used a NIST framework for your IT risk assessment the overlap will be larger.
<https://deandorton.com/wp-content/uploads/2021/03/Untitled-2-1-400x400.jpg>

Will there be audits and compliance testing for both GLBA and the new cybersecurity requirements?

At this point there is not enough information to determine if there will be future audits of compliance like GLBA has, but what the Department of Defense (DoD) has been doing may shed light on this. The DoD has been using a NIST 800-171 self-assessment process for some time. However, due to there not being a reporting requirement or any consequences, the process was ineffective. In 2020 the DoD required a self-assessment with a reporting requirement. At some point between 2021 and 2026, there will be a requirement to have an independent IT audit performed to be certified for compliance. It is not a stretch to think other government agencies will begin adopting this process or something similar. Based on this, the following is what we may see over the course of the next few years.

Self-assessment in 2021

Audit procedures similar to GLBA in 2022 or later

Certification required

When will this impact my institution?

Based on the timeline above, the new cybersecurity requirements will impact your institution this year by way of a self-assessment. The assessment will be reported to the FSA so they can develop a multi-year phased approach to the new cybersecurity requirements. Hopefully the FSA will provide a portal for submitting the self-assessment and a format for doing so. In the meantime, the following self-assessment tool can be used.

[NIST 800-171 Compliance Plan Template](#)

So, the most important question on your list may be, how much work is this going to require? Dean Dorton works with many IHEs and not one of them has extra IT resources to throw at yet another set of compliance requirements. This is going to increase compliance overhead, but following are things that can or will make it an easier pill to swallow.

2021 is just a self-assessment

All of the requirements will not hit in a single year

You've already started if you've adopted any of the NIST frameworks

This will improve your security program

Want more information on other IT Audit and Compliance services? Click the button below:

[IT Audit and Compliance Services](#)

Kevin W. Cornwell
IT Audit Associate Director
kcornwell@ddaftech.com
502.566.1011