

SENATE HELP COMMITTEE
CYBERSECURITY IN THE HEALTH AND EDUCATION SECTORS
TESTIMONY OF HELEN NORRIS

Chair Murray, Ranking Member Burr, and Members of the Committee,

Thank you for holding today's hearing on cybersecurity in the education and health sectors and for providing me with the opportunity to testify about the cybersecurity landscape in the higher education sector. My name is Helen Norris and I am the Chief Information Officer at Chapman University. As the CIO, I am responsible for all technology at the institution and oversee our cybersecurity practice. Chapman is a midsize private university, with about 10,000 students, in Southern California. However, I have worked in higher education across a variety of institutions since 1997, including UC Berkeley, a large research university, and the California State University.

I will focus my testimony today on cybersecurity threats and challenges in the higher education sector, the impact those threats have on a campus community, and the steps that cybersecurity professionals and their colleagues are taking to prevent, mitigate, and respond to these challenges.

Cybersecurity Threats and Challenges in Higher Education

The cybersecurity threat landscape has grown and transformed over the years. Colleges and universities are a target for hackers and need to defend against threats in the form of ransomware, hacking, phishing and social engineering as they manage sensitive data, including student data. We manage personal data pertaining to our employees, and financial data including

payment and banking information. Universities that include medical centers and teaching hospitals face an additional layer of cybersecurity considerations as they also manage personal health information.

It is important to understand that university data systems are highly complex environments to manage and that those systems have both grown in number and data content over recent years. This complexity accelerated even further during the pandemic, as we found ourselves supporting at-home work and a vastly increased online presence in teaching and research. These developments necessitated that we expand our “protection zone” beyond the institution’s network to encompass a national or global workforce and student body. This is all within a diverse technical infrastructure that includes our data centers and third-party partners. Colleges and universities must keep these realities in mind as they evaluate and assess the cybersecurity threats that exist today and the challenges those threats pose to the campus community. The scope and intensity of our data operations presents challenges to keeping them secure, and we know that bad actors are looking every day for ways to turn our difficulties into their opportunities.

I would note that higher education is not monolithic. There are approximately 6,000 Title IV institutions across the country, and there is incredible variety amongst them, including community colleges, research institutions, HBCUs, small private institutions and so on. The challenges related to cybersecurity are different across these institutions, although there are some common themes.

First, the need to address cybersecurity threats is an expensive endeavor, particularly in a sector that faces other budget pressures, such as an across-the-board rise in costs, delays in the post-pandemic recovery of enrollments, and the need to maximize college affordability. It has

become necessary for universities to invest in this area, especially in terms of hiring information security professionals, as well as acquiring security tools and services. This investment varies depending on the type of institution. A large research university or one with a medical center might employ a good-sized information security department. But a smaller university or a community college with more financial limitations simply can't afford to do this, even though they must protect similar information on behalf of their students and their community. In addition to the cost of this operation, cybersecurity is a highly competitive field, and the nation as a whole simply does not have enough human resources currently to meet the demand.

Universities are at a disadvantage in competing with employers in the tech sector when hiring information security professionals, where the jobs are better-paying and seem more attractive. It is difficult for higher education institutions to develop and retain a skilled cybersecurity workforce. One approach we have taken to addressing this challenge is to integrate our students into our workforce, an action that brings benefits for all.

In addition to the human resources needed to manage the risk, the complexity of the work is enormous. We are constantly dealing with new threats but also new and sometimes conflicting regulations and requirements. We have ever-growing lakes of data with privacy implications that must be protected. New threats are introduced with alarming speed, and we must pivot to address them as they arise. To manage these ever-growing threats, a variety of tools are developing in the marketplace. Universities need highly skilled-integration engineers and security experts to blend these tools together and implement the full monitoring, notification, and automated steps taken at each layer of our environment. Over time, we do expect artificial intelligence to improve the ability of these tools to deliver these protective actions more efficiently and independently.

Even more expensive than managing the risk is the cost of addressing an incident when one occurs. Ransomware is now among the most well-known types of security incident. In this situation, a hacker essentially “kidnaps” the victim’s data by encrypting it and will only share the key to decrypt the data when a ransom is paid. While we don’t have exact figures on how often this occurs in any sector, we know that a number of successful ransomware attacks, some very high profile, have occurred at colleges and universities. Ransomware attacks are usually carried out by offshore hackers, which makes addressing them even more challenging. It can be highly lucrative for these individuals, and usually there is very little risk to them with this activity. Ransomware tactics and techniques have continued to evolve in recent years, demonstrating threat actors’ growing technological sophistication and an increased ransomware threat to organizations globally. For example, ransomware threat actors are now using double and triple extortion by threatening to:

1. Publicly release stolen sensitive information,
2. Disrupt the victim’s internet access, and/or
3. Inform the victim’s partners, shareholders, or suppliers about the incident.

Ransomware attacks on universities have been highly disruptive, shutting down the daily operations of the university until the ransom is paid, or the data can be recovered in other ways, a process that usually takes days or weeks. All of this is costly for colleges and universities in financial terms and is also highly disruptive for the institutional community that lacks access to those systems or data during this downtime. An article from the EDUCAUSE review included here as Appendix 1 illustrates some of the impact of a ransomware incident. Quoting from the article: “The impact of a ransomware attack can be devastating. For example, a West Coast university was the victim of a ransomware attack involving data within their school of medicine's

research department. After the university realized hackers had encrypted valuable research data, the school chose to pay the hackers \$1.14 million in cryptocurrency in hopes that the hackers would provide a decryption key. Fortunately, the school reported that it received a key to restore access to the files and copies of the stolen documents. The FBI recommends against ever paying a ransom to ransomware attackers, as there is no guarantee that the data will be recovered, and paying the ransom encourages the hackers to repeat the attack. The FBI encourages victims of ransomware attacks to contact their local FBI field office to request assistance.

Most types of cyberattacks are happening globally. In England, a top university recently suffered a ransomware attack that forced the school to shut down nearly all of its IT systems. The school was forced to delay the start of the next term while IT teams scrambled to investigate the attack and determine the effect on their systems. The impact of ransomware is not always just a monetary loss, as the disruption to a school's term start will affect many other programs and schedules down the road.”

Even when the security teams are successful in avoiding an interruption in services or paying a ransom, hacking incidents are still disruptive and time-consuming. In 2020 a university in California discovered that hackers had infiltrated its systems. While the team successfully shut down the initial attack immediately, they later learned that the cybercriminals had stolen passwords that gave them access to the campus systems for a much longer period.

As in other sectors, higher education is at risk of data breaches, often, as described above, as part of a ransomware attack. In most states, there is a requirement to notify individuals when certain aspects of their personal data have been exposed. This is indeed appropriate. However, it can be an expensive and disruptive process for the institution. In 2017, IBM and the Ponemon Institute

published research that showed that the average cost of a breach that involves data exposure can result in costs to the university of \$245 per record. The financial impact of a significant breach, which may involve hundreds or thousands of records, can be devastating to a university.

Higher education institutions also face a complex regulatory environment in relation to cybersecurity. Recent revisions by the Federal Trade Commission (FTC) to its Safeguards Rule established under the Gramm-Leach-Bliley Act (GLBA) have greatly expanded the number and scope of requirements with which college and university cybersecurity programs must comply starting late this year. These new mandates are all the more pressing since Safeguards Rule compliance is also a condition of the agreement that institutions must sign to participate in Title IV Federal Student Aid programs authorized under the Higher Education Act. The revised Safeguards Rule directives delve deeper than ever before into institutional cybersecurity, applying to systems that are *connected* to systems that contain covered information and specifying particular human resources practices that institutions must adopt in relation to their information security staff, among many other things. While colleges and universities are working hard to meet the FTC's December deadline for compliance, many will certainly be challenged to address the significant expansion of Safeguards Rule requirements by the end of the year.

When releasing the new version of its regulations, the FTC also asked for public comment on a proposal to add an incident reporting requirement to the Safeguards Rule. The FTC has not yet indicated whether a final rule on this issue will be released or what its final form will be if so, but the higher education community was generally satisfied with the proposed regulation as initially presented. However, an additional incident reporting requirement from the FTC would exist alongside state data breach reporting requirements that vary across the 50 states. Higher

education institutions try to account for the current diverse array of reporting laws and regulations by designing institutional incident response and breach notification processes around their common elements. Differences still exist, though, and simply being prepared to track and address those differences in relation to any given incident carries with it significant administrative overhead. Therefore, additional reporting requirements, such as the FTC's proposed incident reporting requirement, that may themselves seem manageable in isolation should be understood as introducing more layers to an already tall stack of compliance measures that institutions have to follow, and those efforts present additional costs with which institutions, as well as students and other stakeholders, have to contend.

Colleges and universities also know that, in addition to complying with the Safeguards Rule, they will eventually be required by the U.S. Department of Education to follow the cybersecurity guidelines for "controlled unclassified information (CUI)" developed by the National Institute of Standards and Technology (NIST). This stems from the fact that "education records" as defined by the Family Educational Rights and Privacy Act (FERPA) are considered CUI under the National Archives and Records Administration (NARA) CUI Program established as a result of Executive Order 13556, "Controlled Unclassified Information." The Office of Federal Student Aid has previously stated that it considers Federal Student Aid data shared with institutions to facilitate the awarding and distribution of federal student financial aid to fall under the "education records" CUI category, and thus it intends to work toward ensuring institutional compliance with the NIST CUI guidelines in the years ahead. Institutions that conduct relevant research for the U.S. Department of Defense (DoD) must already follow these guidelines in relation to the DoD CUI (or covered defense information (CDI)) related to those projects, with

the guidelines also forming an integral part of DoD's Cybersecurity Maturity Model Certification (CMMC) Program. The application of the guidelines to student financial aid information, however, will greatly expand their scope of impact across colleges and universities as well as within institutions, given that the CUI requirements are associated with student financial aid data that will generally find its way into multiple institutional administrative systems. While many institutions have a working knowledge of the NIST CUI guidelines and may in fact be complying with them now, many others know that meeting the standards will be one more resource-intensive exercise on top of compliance efforts, such as fulfilling the new Safeguards Rule provisions, that are already underway. (Please see Appendix 2 for the supporting documents regarding the regulatory issues discussed in this and the immediately preceding paragraphs.)

Colleges and universities take compliance with federal and state cybersecurity requirements very seriously. Beyond regulatory compliance, we take even more seriously our obligation to our students, their families, and our stakeholder communities to secure the data with which we are entrusted and to provide secure environments in which learning, research, and service can take place. The ever-growing number and complexity of the compliance requirements that we face, however, presents an ever-expanding set of administrative burdens and associated costs that may detract from our capacity to manage the actual cybersecurity risks confronting our institutions, both now and in the future. Higher education technology and cybersecurity leaders would welcome the opportunity to explore with policymakers and regulators how these requirements might be streamlined to ensure that we can maximize the value of our cybersecurity resources to maximizing our cybersecurity effectiveness.

Impacts on students, staff, patients and families

Students are also directly and personally impacted by the disruption of an actual breach.

Ransomware attacks can cripple the university's ability to operate by taking down critical systems for an extended period of time, as noted in the earlier example from the United Kingdom. During that time, students lose access to critical services that they need from the institution. This may include the ability to communicate with their faculty as well as the ability to manage their assignments and tests, directly impacting their educational experience. In some instances, colleges and universities have chosen to shut down all services, including canceling classes, until they are confident that they have eliminated the threat from the system or systems in question. Students are also impacted during a data breach if their own data is exposed, creating the risk of negative personal and financial impacts.

Incidents that impact individuals, however, are most often at a smaller scale than a major data breach or ransomware incident. Students in particular must be ever-vigilant to the ongoing attempts by hackers to trap them via email scams based on social engineering. There are many incidents in which a student "falls for" an email scam fraudulently offering a part-time job or threatening to share embarrassing personal information, and the student actually loses money in the process. These phishing attacks involve a hacker impersonating a trusted authority and convincing the victim to share his or her personal information, or even send money to the individual. Students are often victims of a particularly common form of this scam comprised of a fake job offer. In the past we have seen increases in this activity at specific times of the year, such as holidays or tax time, and higher education institutions are often and explicitly targeted.

How colleges and universities prevent, mitigate and respond to these challenges

While the challenges we face are real and complex, the higher education sector is sophisticated in cybersecurity threat mitigation and protection. As noted, most of us have invested resources to build effective cybersecurity capacity. Our information security teams deploy a variety of technologies and processes to protect institutional networks and systems. During the pandemic, as our staff, faculty and students all needed to work, teach, and learn remotely, colleges and universities had the need to implement and extend our technical protections to off-site locations. Some of the technical tools we use to respond to cybersecurity challenges are outlined below:

- Implementing multi-factor authentication to govern system access;
- [End Point Detection and Response Systems \(EDR\)](#), which protects systems both on and off the campus network;
- The use of technology such as firewalls to protect the physical network;
- Encrypting our most sensitive data;
- Network segmentation, which puts our more valuable and sensitive data in a more secure section of the network;
- Addressing software vulnerabilities by applying patches provided by our partners;
- Utilizing virtual private network (VPN) technology to encrypt data when it is accessed from a remote location;
- Using modern monitoring technology to root out suspicious activity on our networks and investigate those activities.

While we often tend to think of cybersecurity as focusing on technical solutions, it is in fact a very human issue and many of the efforts in colleges and universities to combat cybersecurity threats involve outreach to our stakeholders. For example, as previously noted, many security

incidents result from an individual falling into a trap set by a hacker through phishing. Higher education information security professionals strive to ensure that the members of our institutional communities have the tools to protect themselves from such incidents—tools that will help them recognize these traps and avoid them altogether, creating a strong **human** firewall for our institutions. Examples include:

- As noted above, implementing multifactor authentication to govern systems access and educating our community on its importance;
- Phishing campaigns designed to educate our students, faculty and staff on this risk; and
- General outreach and education, which includes sharing information about current threats.

Colleges and universities also address cybersecurity challenges by amplifying our strength through collaboration. As noted previously, there is a great variety in the type of institutions and how they are resourced. Less well-resourced colleges and universities may not individually have the level of human resources needed to manage the range of threats they face on their own. But the overall community comes together to protect the entire ecosystem. Through organizations like EDUCAUSE, Internet2 and REN-ISAC, we share information on new threats, best practices and community-sourced tools. In addition, we work closely with partners in many federal and state agencies, particularly the FBI and CISA. Many institutions develop relationships with their local FBI cybersecurity teams in advance of an incident. This collaboration helps us to avoid problems, and it also enables us to respond more quickly when an incident does occur. CISA offers a variety of free cybersecurity services and tools to colleges and universities, including an online database of known exploited vulnerabilities that is a critical tool, and even free vulnerability scanning. (<https://www.cisa.gov/free-cybersecurity-services-and-tools>) That means

that CISA will test an institution's internet-facing systems to find weaknesses. Literally hundreds of colleges and universities take advantage of these great services, and they are a critical part of our defense.

Finally, while we plan and protect, universities also prepare for the worst using several different techniques. Most universities have created incident response plans (IRPs) that outline what we should do in the event of a cybersecurity incident such as a ransomware attack. Universities generally test these plans on a regular basis via tabletop exercises that allow them to evaluate their preparedness for an event and adjust their plans as necessary. Some institutions also carry cyber insurance that aids them in the event of an incident, with their insurance carriers also providing guidance in the preparation and testing of an IRP. Unfortunately, cyber insurance has become prohibitively expensive for some institutions, and looking to the future, the growing cost of cyber insurance remains a concern for higher education as a whole.

In summary, colleges and universities usually take a multi-layered approach to security by:

- Utilizing technical tools to protect our networks and technical environments from unauthorized access by hackers;
- Using outreach, communication and education to protect our institutional communities from phishing for data and credentials, email scams and ransomware;
- Actively engaging with federal agencies and the higher education community in general to increase our own awareness of current threats and risks, allowing us to avoid becoming a victim of those new threats; and
- Preparing and planning for an incident should one occur.

In conclusion, I would again like to thank the Committee for your attention to this important issue. I look forward to continued collaboration and conversation on this topic.

APPENDIX 1

Why IT Matters to Higher Education

EDUCAUSE
REVIEW

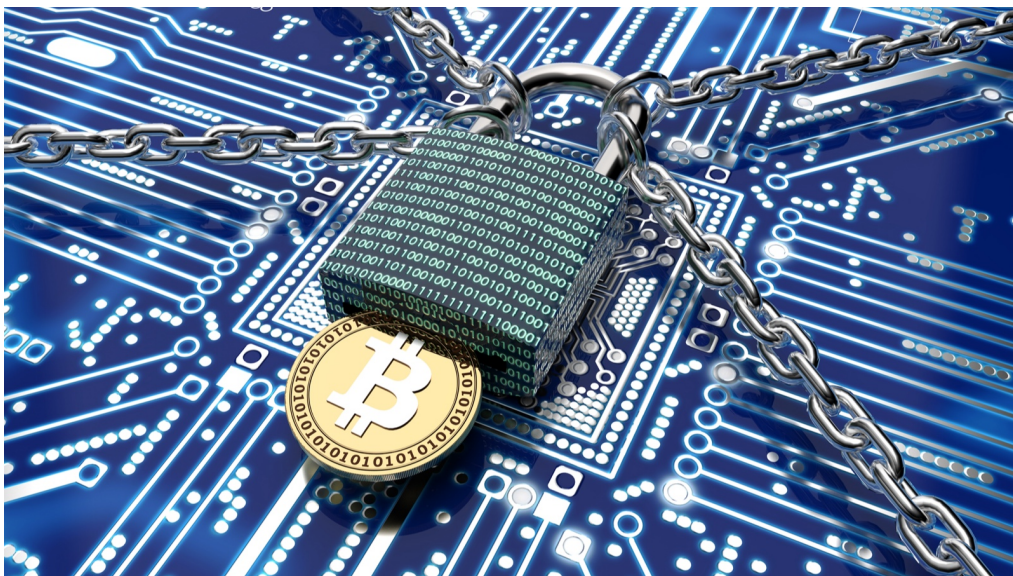
The Increasing Threat of Ransomware in Higher Education

Steve Scholz, William Hagen and Corey Lee Tuesday, June 22, 2021

Cybersecurity and Privacy

7 min read

Cyberattacks are increasing in frequency and impact. Defending against ransomware attacks requires a tiered approach to security with a Zero Trust model at the heart of the methodology.



Credit: posteriori / Shutterstock.com © 2021

During the pandemic, several major cyberattacks have unfolded, resulting in severe impacts to organizations and individuals. One of the most talked-about cyberattacks in 2020 was the SolarWinds breach, in which hackers gained access to nearly 18,000 clients of SolarWinds. The victims of the attack include Fortune 500 companies and multiple US government agencies.

In May 2021, Colonial Pipeline Company, a major refined-oil products supplier responsible for 45 percent of the East Coast's fuel supply, was hit in the largest-known hack to date on US energy infrastructure. The attack caused Colonial Pipeline to shut down its entire system, leading to panic and a disruption in gasoline supply across the East Coast of the United States.¹ In order to unlock encrypted files and get the pipeline back up and running, Colonial Pipeline paid hackers \$4.4 million in Bitcoin for a decryption key.

Recently, the number of ransomware attacks similar to the attack on Colonial Pipeline has increased dramatically. The number of ransomware attacks more than doubled as cybercrime operations increased throughout the coronavirus pandemic. These attacks grew not only in frequency but also in sophistication and ransom demand. In 2018, the average ransom demanded from a victim was \$8,000. In 2020, the average demand grew to \$170,000, with high-end demands exceeding \$1 million.²

Ransomware attacks are not only affecting businesses; colleges and universities are also prime targets for attacks. Surprisingly, education is the most affected sector for malware attacks when compared to other industries like business and professional services, retail and consumer goods, and high tech. Within the last thirty days, educational organizations have been the target of more than 6.1 million malware attacks, while the second-most affected industry (business and professional services) has only seen 900,000 attacks.³ An analysis of ransomware campaigns within higher education found that ransomware attacks against colleges and universities have more than doubled since the onset of the coronavirus pandemic.⁴

The FBI's Cyber Division recently warned that ransomware poses a huge risk for higher education, as cybercriminals using this type of attack are now focusing heavily on colleges and universities.⁵ The FBI became aware of a new type of ransomware attack—using a new type of malware known as PYSAs—where unidentified cyber actors are specifically targeting higher education, K–12 schools, and seminaries. These actors use PYSAs to exfiltrate data from victims prior to

encrypting the victims' systems to use as leverage in eliciting ransom payments.

What Is Ransomware?

Ransomware is a malicious form of malware, where hackers deploy a malicious computer code to block an organization's access to its own computer network to extort a ransom. The types and complexity of ransomware attacks have increased rapidly over time, and today many ransomware attacks see cybercriminals gaining access to an organization's data and then holding it hostage with military-grade encryption.

There are three main types of ransomware (listed below in order of increasing severity and complexity):

- **Scareware:** This type of ransomware typically includes rogue security software and tech-support scams. In this type of ransomware, the victim may receive a pop-up message claiming that malware was discovered on their system, and the only way to eradicate the malware is to pay for the security software to remove it. In most cases, this type of attack poses little actual risk to files and data.
- **Screen lockers:** When a screen locker attack is deployed, the victim is locked out of their computer entirely. Upon startup, a full-size window will appear demanding ransom payment and prohibiting the victim from using their computer.
- **Encrypting ransomware:** This is the most complex and devastating type of ransomware. Cybercriminals will gain access to the victim's system, seize their files,

encrypt them, and then demand payment for decrypting and returning the files.

When faced with an encryption ransomware attack, the victim is left with only a few choices: they can either pay a ransom to the criminals (which does not guarantee the criminals will return the data), attempt to break the encryption on their data, or restore their data and systems from backups.

In a ransomware attack, hackers typically search out an organization's most valuable data. High-profile ransomware attacks sometimes target organizations that are conducting research where the data is highly confidential. In other cases, the data the attackers might be after could be confidential data about a university's students, including social security numbers, addresses, and birthdates. Another common target for ransomware attacks is any type of data or system that could make it impossible for an organization to function. Because of the data they possess, higher education institutions are key targets for ransomware attacks.

However, even smaller universities and colleges, as well as those without an emphasis on research, are prime targets for this type of cyberattack. Regardless of whether an institution considers its data to be valuable, chances are that cybercriminals do. Higher education institutions inherently gather and store large amounts of confidential student data and therefore must protect themselves against ransomware attacks.

Even more concerning than traditional malware-based ransomware attacks are human-operated ransomware attacks,

which pose a huge threat to organizations of all types. An advanced type of ransomware, human-operated ransomware attacks are becoming more frequent and costly. In a human-operated attack, a cybercriminal is actually controlling the attack in real-time, and after gaining access to a victim's system, the criminal quickly scans through files and locations—while also preventing any antivirus alerts—to pinpoint and steal the most valuable data.

In these types of attacks, the attacker will often exhibit extensive knowledge of systems administration and common network security misconfigurations, perform thorough reconnaissance, and adapt to what they discover in a compromised network. Existing antivirus solutions are often not a strong enough defense when an organization is faced with this type of hands-on-keyboard ransomware attack.

The Impact of Ransomware Attacks

The impact of a ransomware attack can be devastating. For example, a West Coast university was the victim of a ransomware attack involving data within their school of medicine's research department. After the university realized hackers had encrypted valuable research data, the school chose to pay the hackers \$1.14 million in cryptocurrency in hopes that the hackers would provide a decryption key. Fortunately, the school reported that it received a key to restore access to the files and copies of the stolen documents. The FBI recommends against ever paying a ransom to ransomware attackers, as there is no guarantee that the data

will be recovered, and paying the ransom encourages the hackers to repeat the attack. The FBI encourages victims of ransomware attacks to contact their local FBI field office to request assistance.

Most types of cyberattacks are happening globally. In England, a top university recently suffered a ransomware attack that forced the school to shut down nearly all of its IT systems. The school was forced to delay the start of the next term while IT teams scrambled to investigate the attack and determine the effect on their systems. The impact of ransomware is not always just a monetary loss, as the disruption to a school's term start will affect many other programs and schedules down the road.

Developing a Strategy to Help Prepare for Ransomware Attacks

Defending against ransomware attacks requires a tiered approach to security with a **Zero Trust model** at the heart of the methodology. So, how does Zero Trust work? Zero Trust follows three guiding principles: verify explicitly, use least privileged access (LPA), and assume breach.

- **Verify explicitly:** Zero Trust closes gaps in multi-factor authentication (MFA) coverage by requiring explicit verification across the network. Instead of assuming trust based on weak assurances like network locations, Zero Trust uses all available data—identity, endpoint, and network data—to authenticate all access requests,

no matter where they came from or what they're accessing.

- **Use least privileged access (LPA):** Zero Trust makes it harder for attackers to negatively impact key systems and data by limiting users' access to the resources, devices, and environments they need. Without widespread privileges and access, attackers have fewer opportunities to move laterally within the network beyond an initial breach.
- **Assume breach:** As a final fail-safe, Zero Trust operates under the assumption that a breach has already happened or soon will. This means deploying redundant security mechanisms, collecting system telemetry, using that telemetry to detect anomalies, and—wherever possible—automating insight generation to enable near-real-time prevention, response, and remediation.

IT professionals play an important role in security and are the foundation of an approach to preventing ransomware. Many observed ransomware attacks leverage malware and tools that are easily detected by antivirus security software. Observed affected servers also often lack firewall protection and MFA, have weak domain credentials, and use non-randomized local admin passwords.

Oftentimes, these protections are not deployed because there is a fear that security controls will disrupt operations or impact performance. IT professionals can help determine the true impact of these settings and collaborate with security teams on mitigations. Attackers often prey on settings and configurations that many IT admins manage and control. Given

the key role they play, IT professionals should be part of security teams to defend against ransomware attacks.

When considering complex, human-operated ransomware attacks, traditional solutions like MFA and antivirus are a good start but will not completely defend an organization against a knowledgeable cyberattacker. The only way to defend against these types of events is a twofold approach involving top-of-the-line endpoint detection and response paired with a user entity behavior analytics (EUBA) solution. This is the only way to pinpoint if there is an attacker on the inside of a system who has managed to evade or silence antivirus alerts.

Microsoft has the tools and expertise needed to ensure your security system is able to prevent ransomware attacks.

Contact your Microsoft account representative to discuss your security needs and learn how higher education institutions are defending against ransomware attacks.

Additionally, you can learn more about Microsoft's approach to defending against these types of cyber-attacks and **human-operated ransomware on Microsoft Docs.** [↗](#)

Notes

1. Will Englund and Ellen Nakashima, "**Panic Buying Strikes Southeastern United States as Shuttered Pipeline Resumes Operations,**" [↗](#) *Washington Post*, May 12, 2021. [↶](#)

2. John Leyden, "**Ransomware Attacks More Than Doubled Last Year as Cybercrime Operations Scale Up during Coronavirus Pandemic,**" [↗](#) The Daily Swig (website), March 8, 2021. [↩](#)
 3. Microsoft Security Intelligence, **Global Threat Activity Map by Industry,** [↗](#) Microsoft (website), accessed June 4, 2021. [↩](#)
 4. **Cybersecurity in Higher Education,** [↗](#) research report, (New York, NY: BlueVoyant, February 2021). [↩](#)
 5. Federal Bureau of Investigation Cyber Division, **Increase in PYSA Ransomware Targeting Education Institutions,** [↗](#) FBI FLASH, Alert Number CP-000142-MW, March 16, 2021. [↩](#)
-

Steve Scholz is Principal Technical Specialist for Security, Compliance and Identity, US Education, at Microsoft.

Bill Hagen is a Senior Director of Security addressing industry, partner, and customer requirements at Microsoft.

Corey Lee is Senior Consultant and Zero Trust Architect at Microsoft.

Microsoft is a supporting partner of EDUCAUSE.

© 2021 Microsoft.

- **Cyber Threat Intelligence, Cybersecurity, Encryption, Endpoint Detection and Response (EDR), Incident Management and Response, Intrusion Detection and Prevention, Security Risk Management, Vulnerability Management, Zero Trust**

APPENDIX 2

Why IT Matters to Higher Education

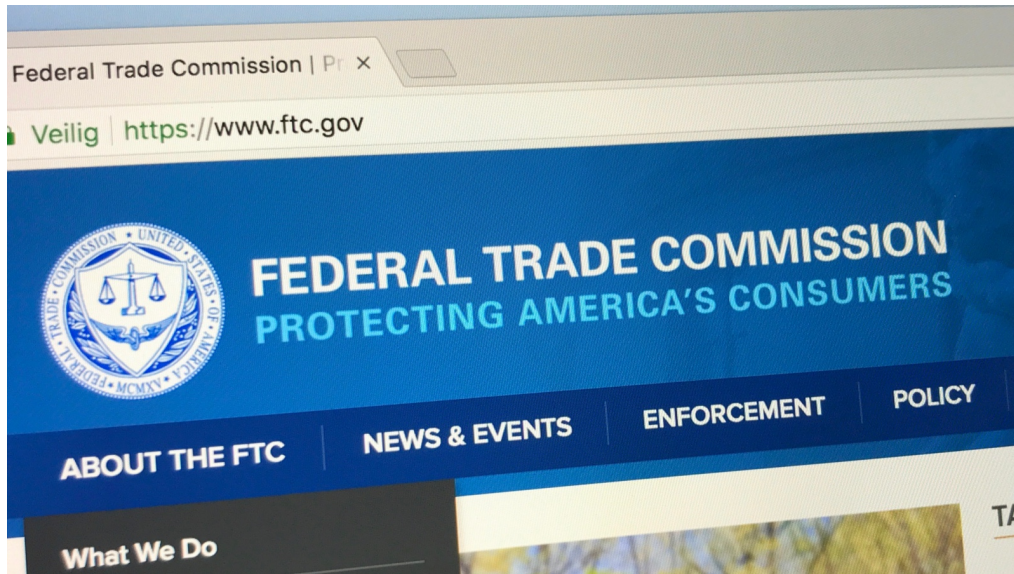
EDUCAUSE
REVIEW

Policy Analysis: Revised, Highly Prescriptive FTC Safeguards Rule

Jarret Cummings Thursday, December 2, 2021 **Policy**


20 min read

The Federal Trade Commission (FTC) has released a revised version of the Safeguards Rule. The revised Rule will impose many new requirements on institutional cybersecurity operations in relation to student financial aid and other "customer" information.



Credit: Jarretera / Shutterstock.com © 2021

Note: The Federal Trade Commission officially published its revised Safeguards Rule in the *Federal Register* on December 9, 2021, making December 9, 2022, the deadline for institutions to achieve compliance with the new requirements of the revised Rule. **The text below has been updated as of March 9, 2022, to reflect this change.** Some of the document links have been revised as well to reflect new, post-publication locations of the respective resources.

When the Federal Trade Commission (FTC) proposed to **revise**  the Safeguards Rule (the Rule) in 2019, EDUCAUSE joined with the American Council on Education (ACE) and several other associations to submit **comments** asking for a number of changes and clarifications.¹ Those comments derive largely from an **analysis** (written by EDUCAUSE members and staff) of the FTC's proposed revisions to the Rule.² In light of the

initial comments that the FTC received, including ours, the agency held an online listening session during the summer of 2020. Among the select stakeholder panelists the FTC invited to participate were a few EDUCAUSE member CIOs and CISOs. However, the FTC did not provide any insights into how the feedback it received on its proposed rulemaking might influence the form that its revised cybersecurity regulations would take. The agency **released** [↗](#) the latest version of the Safeguards Rule on October 27.³ This version is largely unchanged from the FTC's original draft. *(Note: The pre-publication draft originally made available by the FTC on October 27, 2021, was replaced by a pre-publication version posted to the online version of the Federal Register on December 8, 2021. The references and links to the pre-publication draft of the revised Rule have been updated to reflect the December 8 version in the online Federal Register since that is the pre-publication form of the document still available. The same is true for the supplemental notice of proposed rulemaking regarding a possible Safeguards Rule reporting requirement. The December 8 version of that document is the pre-publication version still available, so relevant references and footnotes have been updated accordingly.)*

Given the extensive edits, clarifications, and changes that we requested,⁴ the FTC's decision not to substantially revisit its regulatory proposal is disappointing. That said, the analysis of public comments provided with the FTC's **pre-publication copy** [↗](#) of the new Rule contains an important acknowledgment from the agency that sets the context for interpreting and applying the numerous provisions with which colleges and universities will now have to comply:

Although the Final Rule has more specific requirements than the current Rule, it still provides financial institutions the flexibility to design an information security program that is appropriate to the size and complexity of the financial institution, the nature and scope of its activities, and the sensitivity of any customer information at issue.⁵

This statement is significant because it is relevant to a point that EDUCAUSE and our higher education association partners pressed throughout our comments on the proposed Rule. We consistently noted that many provisions lacked sufficiently specific guidance to assure a college or university that it had achieved compliance, an issue that we summarized as follows:

The proposed revised Rule, however, specifies many of the details of those elements while adding more provisions and requirements, but without providing effective guideposts for compliance. That leaves colleges and universities with many questions about whether the proposed Rule's provisions are appropriately limited to the data and functions it covers and how institutions will effectively be able to determine if they are in compliance regardless.⁶

The statement from the FTC quoted above directly addresses this concern.⁷ In my view, it reaffirms that an effective approach to the requirements of the Safeguards Rule, including all of its new provisions, remains a matter of discretion for the covered entity in question based on its size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. The Rule identifies the elements that an institution's information security

program must include; however, it leaves the determination of how the institution should address those elements (for the most part) to the covered entity, with the understanding that the institution will make those decisions based on, and reasonably justified by, its particular context.

From a compliance standpoint, institutions may view this level of discretion as a double-edged sword based on understandable concerns about their decisions being second-guessed by regulators at some point in the future. Given the FTC's position as reflected in the acknowledgment from the agency quoted above and its analysis of public comments on the proposed revisions to the Rule, institutions may best respond by adopting an approach that EDUCAUSE asked the FTC to affirm explicitly in the Rule or its related guidance (which it apparently declined to do in favor of reaffirming the extent of institutional discretion):

[W]e would urge the FTC to explicitly state in the Rule and subsequent guidance what we believe the proposed revised Rule implies—that institutions may achieve compliance through providing reasonable explanations in their information security program documentation for the choices they make in fulfilling the given provisions.⁸

In other words, the discretion to determine what constitutes an appropriate way to fulfill a given requirement based on an institution's size and complexity, the nature and scope of its activities, and so forth carries with it the responsibility of ensuring that the measures adopted by the institution are appropriate given what it is, what it does, and what options it may reasonably have available to it as a result.

I used the word "regulators" above, not "the FTC," because the Office of Federal Student Aid (FSA) at the US Department of Education (ED) has made compliance with the FTC Safeguards Rule a requirement of the Title IV Program Participation Agreement (PPA) that institutions must sign to participate in federal student financial aid programs.⁹ As a result, institutions are ultimately responsible to the FTC directly for complying with the Safeguards Rule, but a determination by FSA that an institution is not complying with the Safeguards Rule may affect its Title IV eligibility and therefore the ability of the students enrolled at the institution to get federal student loans and other forms of federal financial aid.

It remains unclear how FSA will address the changes in the FTC's cybersecurity regulations. Conversations between EDUCAUSE and FSA representatives about the issues that have occurred since the FTC unveiled its rulemaking notice in 2019 did not produce any indication of how FSA would incorporate Safeguards Rule revisions into its compliance expectations. For now, the **Safeguards Rule audit objective** that FSA had incorporated into the federal single audit process still focuses on confirming a few high-level objectives from the previous version of the Rule:

- That an institution has appointed a person or team to coordinate its information security program
- That it has conducted a relevant risk assessment
- That it has developed information security controls based on its identified risks¹⁰

FSA will have to work with the Office of Management and Budget to alter the audit objective in light of the FTC's revisions to the Rule, if and when it chooses to do so, and that process will take time.

Meanwhile, EDUCAUSE intends to work with its members and association partners to engage with FSA to understand its Safeguards Rule compliance and audit objective plans as they take shape. We hope such discussions will also provide the opportunity for member representatives to share information about the practical issues and difficulties that different approaches to FSA compliance in this area might present. In this regard, FSA is better positioned to understand the problems that the revised Rule creates for colleges and universities and to tailor its compliance interests to the higher education context.

Turning to the revised Rule itself, even with the understanding that how an institution fulfills a given requirement remains discretionary, the long list of new requirements is still eye-opening. Also, the FTC is now requiring the adoption of several measures that EDUCAUSE argued in 2019 should continue to fall under institutional discretion. In the review that follows, I highlight what I consider to be key points in the revised Rule. I encourage EDUCAUSE members involved in their institution's compliance with the Safeguards Rule to review the **revised regulations** [↗](#) in their entirety (see pp. 109–128 for the text of the new Rule itself), as some parts of the Rule may be more central to your institution's needs and interests than the ones I identify below.

In addition to releasing the revised Safeguards Rule, the FTC also announced that it would conduct a **supplemental**

rulemaking [↗](#) on the issue of whether to require entities covered by the Rule to report relevant cyber incidents to the FTC.¹¹ The higher education comments on the proposed Rule that EDUCAUSE helped to develop in 2019 raised questions about the value of such a reporting requirement, especially as it relates to the burden that the requirement would create for covered entities such as colleges and universities. The new FTC rulemaking notice indicates the agency's desire to minimize the potential burden of Safeguards Rule incident reporting, which may, in turn, lessen higher education's concerns about a proposed requirement. I will be writing a supplemental article in which I review the need to consider whether EDUCAUSE and the higher education community should submit comments on the FTC's proposed incident reporting requirement and, if so, the direction those comments should take. *(Note: The review of the rulemaking notice regarding a possible Safeguards Rule reporting requirement was posted on **December 8, 2021**. EDUCAUSE joined several associations in submitting comments about the proposed reporting requirement to the FTC on February 7, 2022. An article reviewing the higher education submission, with a link to the comments themselves, was posted on **March 3, 2022**.)*

The Revised FTC Safeguards Rule: Key Provisions by Section

Please note that the *Code of Federal Regulations (CFR)* reference for the Safeguards Rule is **16 CFR 314**. [↗](#) To find the Safeguards Rule regulations, enter "16 CFR 314" in the search bar on the **Electronic Code of Federal Regulations** [↗](#) web page.

Section 314.5—Effective Date

Keep in mind that most of the new requirements added to the Rule will not take effect until one year after the date of their publication in the *Federal Register*. (Note: The revised *Safeguards Rule* was officially published in the *Federal Register* on December 9, 2021, and it identifies December 9, 2022, as the compliance deadline for the new requirements incorporated into the revised Rule.) With that in mind, I will take the second-to-last section, Section 314.5—Effective Date, out of order since it identifies the following sections as falling under the one-year compliance deadline:

- 314.4(a)—Designate a "qualified individual" to oversee, implement, and enforce the institution's information security program.
- 314.4(b)(1)—Produce a written risk assessment about the institution's customer information that includes a now-mandated set of criteria and requirements.
- 314.4(c)(1)-(8)—"Design and implement safeguards to control the risks you identity through risk assessment," including the following:
 - Technical and physical access controls to ensure only authorized access
 - An inventory of all relevant parts of the IT environment and management of the same consistent with their business priority and the institution's risk strategy
 - Encryption of all customer information in transit over external networks and at rest

- Procedures for securely developing internal applications and assessing the security of externally developed applications used in relation to customer information
 - Multi-factor authentication for *any* individual accessing *any* information system
 - Procedures for the secure disposal of customer information that is no longer needed for business operations or another legitimate business purpose
 - Change management procedures
 - Measures to monitor and log the activities of authorized users and to detect their unauthorized access or use of or tampering with customer information
-
- 314.4(d)(2)—Implement continuous monitoring of "information systems" (as defined in 314.2) or annual penetration testing with vulnerability assessments at least every six months.
 - 314.4(e)—Establish policies and procedures to ensure that your staff receives security awareness training, that you hire qualified information security personnel and provide ongoing professional development for them, and that key members of your information security staff maintain their knowledge of current threats and responses.
 - 314.4(f)(3)—Periodically assess the information security risks that your institution's service providers present and the adequacy of the safeguards they

deploy to ensure that they are following the provisions of the Rule.

- 314.4(h)—Establish a written incident response plan, including a set of specific elements, for the customer information that the institution controls.
- 314.4(i)—Require your institution's "qualified individual" to submit a written report on key aspects of the information security program to the institution's governing board at least once per year.

All other aspects of the revised Rule take effect thirty days from its publication in the *Federal Register*, but those aspects essentially concern the current requirements of the Safeguards Rule with modest text edits to accommodate the range of new requirements that will go into effect next year. In other words, the thirty-day deadline for the rest of the revised Rule ensures that covered entities continue to comply with pre-existing requirements while preparing to comply with the new ones. *(Note: The revised Rule officially took effect on January 10, 2022; as mentioned, though, the FTC has deferred compliance with the new requirements added to the Safeguards Rule until December 9, 2022.)*

Section 314.2—Definitions

- The FTC greatly expands the definitions section—largely to incorporate key terms from its Privacy Rule directly into the revised Safeguards Rule. These terms are important for understanding what the Safeguards Rule covers.

- For example, where the current regulation includes only the definition of "customer information," the revised Rule includes definitions of terms ("consumer," "customer," "nonpublic personal information," "personally identifiable financial information," and so forth) that are central to understanding what "customer information" actually means.
- EDUCAUSE and its partners specifically requested that the FTC add all relevant definitions from the Privacy Rule to the new Safeguards Rule to make it easier for institutions to understand what "customer information" they need to protect under the Rule, so this change, even at the expense of the Rule's brevity, is greatly appreciated.
- That said, IT leaders and professionals will likely be well served by working with institutional legal counsel as well as their business offices, registrars, and financial aid colleagues to walk through the interlocking chain of definitions that have to be explored to reach a full understanding of exactly what institutional data constitutes "customer information."
- Since institutions currently must comply with the existing version of the Safeguards Rule, most, if not all, probably already have a good handle on the scope of "customer information." However, with all of the relevant definitions now being included in the Rule itself, evaluating

the new compliance requirements presents a good opportunity to review the previous determinations to ensure nothing has been missed.

- **"Authorized user"**

In the revised Rule, the FTC added "customer" to the definition's list of people who might be considered "authorized users" to make clear that the Rule's requirements for multi-factor authentication and user activity monitoring and logging, for example, extend to "customers" that can access their information via the institution's systems.

Depending on how an institution already allows students to access their financial aid and institutional account information, the Rule's new security requirements may or may not pose problems. However, institutions will have to review those requirements in light of students' (or parents') access to account information and make sure all of the required measures are in place in ways that are appropriate to the institution's size, complexity, and so forth.

- **"Encryption"**

In commenting on the proposed Rule, EDUCAUSE and its partners suggested that the FTC add to the definition of "encryption" to link the potential new encryption requirement under the Rule to "industry standards," which would give institutions a frame of reference for complying with the requirement. Instead, the final version of the revised Rule includes a

reference to "current cryptographic standards" as an appropriate measure to secure an associated encryption key.

From a compliance standpoint, I think the end result is the same. In deciding what form of encryption to deploy to meet the Rule's requirement, institutions should document how the method(s)/tool(s) that are chosen reflect current encryption standards and approaches.

- **"Information system"**

As previously mentioned, one of the key definitional changes from the proposed Rule to the Final Rule is the addition of references to "containing customer information or connected to a system containing customer information" in the definition of "information system." As a result, the definition now clearly links systems and related technology covered by the revised Rule's requirements to the customer information for which institutions are responsible under the Safeguards Rule. However, as also noted previously, the addition of "connected to a system containing customer information" likely pulls a much greater degree of an institution's IT environment into the scope of the Rule's requirements than a college or university would find helpful or, in many cases, justified.

This definitional change may point the way, though, to how an institution can modify its IT environment to segregate its "customer information" (with student financial aid and account information likely drawing the lion's share of concern) to limit the extent of the

environment that will fall under the Rule's new requirements, such as continuous monitoring or annual penetration testing or biannual vulnerability assessments. There is little doubt, however, that the FTC did not take into account our points about the extent to which student financial aid information might reasonably be distributed across institutional systems and, therefore, the difficulty that the scope of compliance in the revised Rule might pose for a college or university.

Section 314.4—Elements [of a Safeguards Rule-Compliant Information Security Program]

- **"Qualified individual" to oversee/enforce the information security program [314.4(a)]**

The revised Rule follows the proposed Rule in moving from requiring that an employee or employees be designated to coordinate the institution's information security program to mandating that a single "qualified individual" be appointed to oversee, implement, and *enforce* the program. In our comments on the proposed Rule, we argued that the decision of whether to have individual or team leadership of an institution's information security program should remain a matter of institutional discretion given the great variety of institutional contexts. The FTC determined, however, that streamlining and ensuring accountability by having a single head of the information security program trumped other considerations.

That said, we also noted in our comments on the proposed Rule that the FTC's repeated reference to a chief information security officer in this context, which the agency intended to be just an example, would likely be interpreted as a mandate that all institutions might not be able to address within the anticipated timeframe for achieving compliance. With our feedback and similar comments from other stakeholders in mind, the FTC adjusted its text in the final rule so that it only refers to the need for an institution to appoint a "qualified individual" to lead the information security program. What constitutes being "qualified" will remain subject to institutional discretion based on the institution's size and complexity, the nature and scope of its operations, and so forth.

- **Risk assessment [314.4(b)]**
 - Under the revised Safeguards Rule, institutions will now have to develop a written risk assessment regarding the security of their customer information. The written assessment will have to cover the following elements:
 - The criteria used to evaluate and classify the relevant security risks that the institution has identified
 - The criteria used to assess "the confidentiality, integrity, and availability of your information systems and customer information, including the adequacy of the existing controls in the

context of the identified risks or threats you face"

- The ways in which "identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks"
- The expanded risk assessment requirement in the revised Rule also mandates that institutions periodically update their risk assessments, with when and how to do so left to institutional discretion based on institutional size, complexity, nature, scope, etc.
- **Safeguards [314.4(c)]**
 - The revised Rule goes into much greater detail about the types of security measures that institutions will need to implement to address the risks they identify in their risk assessments. In fact, one could interpret the specific requirements introduced as the FTC setting minimum baselines under the assumption that any valid risk assessment would identify the risks requiring the measures that the FTC is now imposing by regulation.
 - Under the revised Rule, institutions must take the following actions:
 - Implement and maintain technical and physical access controls on customer information to limit access to authorized

users and limit those users' access to the scope of their authorizations.

- Inventory and manage "the data, personnel, devices, systems, and facilities" central to their operations in light of their priority and the institution's "risk strategy."
- Encrypt all customer information "held or transmitted" by the institution when "in transit over external networks or at rest."
 - The FTC had previously raised the possibility of requiring encryption of customer information while in transit over *internal* networks as well, so this encryption provision could have been even more cumbersome to manage.
 - The provision also allows for institutions to use "effective alternative compensating controls" when necessary if approved by their "qualified individual."
- Adopt secure development practices for any internally developed applications and security assessment procedures for any externally sourced applications that

the institution uses to "transmit, access, or store customer information."

- **"Implement multi-factor authentication for any individual accessing any information system** [emphasis added], unless your Qualified Individual has approved in writing the use of reasonably equivalent or more secure access controls."
- Establish policies and procedures for the secure disposal of customer information "no later than two years after the last date" on which the information was used to serve the customer in question unless it is needed for business operations or "for other legitimate business purposes."
 - The institution may also maintain the data if required by law or regulation, or if it is held in a fashion that makes "targeted disposal . . . not reasonably feasible."
 - In responding to the proposed Rule, EDUCAUSE and its partners argued that "business purposes" might not be understood as the FTC intended in institutions focused on academic purposes, and thus it

should use the phrase
"legitimate purposes."

- Since the FTC did not take our suggestion, institutions will have to rely on their discretion based on their size, complexity, nature, scope, etc., to determine what constitutes a "legitimate business purpose" given their operations.
- Also, this provision assumes that secure disposal of customer information as required will be based on a periodically reviewed and updated institutional data retention policy designed "to minimize the unnecessary retention of data."
- Adopt change management procedures (presumably for systems, policies, processes, etc., that connect in some meaningful way with customer information).
- Implement measures to "monitor and log the activity of authorized users" and to detect when they have accessed, used, or tampered with customer information outside the scope of their authorization.

- The logging aspect of this provision replaces a separate provision in the proposed Rule that would have required the creation of "audit trails . . . to detect and respond to security events."
 - EDUCAUSE member feedback indicated that simply focusing on user logs would be a more accurate and useful way to address the FTC's concern, and it seems that our comment about the issue in relation to the proposed Rule led to an appropriate change.
- **Monitoring and testing safeguards [314.4(d)(1) and (2)]**
 - Part 1 of this provision requires institutions to test regularly or otherwise monitor the effectiveness of the safeguards established under their information security program "including those to detect actual and attempted attacks on, or intrusions into, information systems" as defined by the Rule.
 - Part 2, however, specifically mandates either continuous monitoring of information systems (again, as defined by the Rule) or annual penetration testing with vulnerability assessments at least every six months and

whenever the institution experiences significant operational changes or an incident that "may have a material impact on [the institution's] information security program."

- In commenting on the proposed Rule, EDUCAUSE and its partners argued that if, when, where, and how these measures might be deployed should be a matter of institutional discretion based on the findings of the institution's risk assessment in light of its size, complexity, nature, scope, etc., especially given the diversity of institutional types and contexts across higher education.
 - In light of how the Rule defines "information system," limiting the reach of this provision across the institutional IT environment will require careful consideration of where and how customer information is stored and used, as well as which systems and data stores have to be connected to systems and databases containing customer information.
- **Human resources policies and procedures related to information security [314.4(e)]**
 - This aspect of the revised Rule requires institutions to provide security awareness training for their personnel consistent with the results of their risk assessments.
 - Institutions must also do the following:
 - Use qualified information security personnel to manage security risks and

"perform or oversee" their information security program, whether such personnel are institutional employees or are supplied by a service provider.

- Ensure their information security personnel have access to security updates and training that will allow them to address security risks at their institution.
- Verify that "key information security personnel" are maintaining their professional knowledge of the field (i.e., of "changing information security threats and countermeasures").

- **Service provider oversight [314.4(f)]**

The revised Rule adds a requirement that institutions periodically review the information security risks that their relevant service providers pose, including the adequacy of those providers' safeguards.

- **Evaluation and revision of the information security program [314.4(g)]**

The FTC changed this section from the proposed rule to the final rule to cross-reference the requirement about reviewing and revising the institutional information security program with the sections on modifying relevant safeguards based on the results of the institution's written risk assessment [314.4(b)(2)] and its continuous monitoring/annual penetration testing (with at least biannual vulnerability assessments) of relevant information systems [314.4(d)].

- **Written incident response plan [314.4(h)]**
 - The FTC revised this provision slightly in the revised Rule from how it was presented in the proposed Rule.
 - Rather than saying that covered entities have to develop written incident response plans to cover customer information in their "possession," the text now reads that they must have incident response plans for such information under their "control."
 - This edit responds to our comment on the proposed Rule regarding the need to revise this provision to reflect institutional use of cloud services, where the relevant information may actually be possessed by a cloud services provider and not by the institution directly.
 - Whether "control" works better than "possession" in this context remains debatable. We suggested that the text tie the incident response plan to the customer information for which the institution is "responsible," since there is little doubt that the covered entity remains responsible for the security of its data no matter where it is housed, especially in light of the Rule's service provider oversight provision.
 - To that end, regardless of how the text reads, the FTC's intent is clear: The

institution's incident response plan regarding covered customer information must account for relevant service providers as well.

- The provision identifies several specific items that a compliant incident response plan must include, all of which are consistent with standard incident response principles and practices.
 - Institutions with incident response plans that cover customer information should review the list to establish a crosswalk between their plans and the required elements. Those needing to develop such plans should review the list to ensure that their plans cover all the bases.
- **Board reporting [314.4(i)]**
 - The revised Rule incorporates the proposed Rule requirement that the head of the institution's information security program submit a written report about the program to the institution's governing board at least once a year.
 - The modest edits to the provision in the revised Rule identify the head of the information security program as its "qualified individual" and specify that written reports should be provided to the board "regularly and at least annually."

- A Rule-compliant board report must include the following elements:
 - A review of the program's overall status and compliance with the Rule
 - "Material matters" about the program, such as:
 - risk assessment and risk management/control decisions;
 - service provider arrangements;
 - results of testing and security events or violations, and management's responses to them; and
 - recommendations for program changes.

Section 314.6—Exceptions

- Institutions that maintain customer information on fewer than 5,000 consumers (note the difference between "consumer" and "customer" in the definitions) are exempt from having to:
 - develop a written risk assessment [314.4(b)(1)];
 - implement continuous monitoring or penetration testing/vulnerability assessments of their information systems [314.4(d)(2)];
 - develop a written incident response plan [314.4(h)]; or

- submit a report about their information security program to their governing board or senior executive [314.4(i)].
- In commenting on the proposed Rule, EDUCAUSE and its partners argued that the threshold for exceptions to the requirements of the Rule for higher education institutions should be set by Carnegie classification, not the number of consumer records managed, as Carnegie classification would provide a more appropriate indicator of institutional size (and therefore institutional capacity to manage the requirements in question). With the FTC declining to accept that recommendation, even the smallest accredited colleges and universities are unlikely to qualify for the exceptions to certain Rule requirements given the length of time for which financial aid and student account information is generally maintained.

Notes

1. Federal Trade Commission, "**Standards for Safeguarding Customer Information (Notice of Proposed Rulemaking; Request for Public Comment)**," [↗] *Federal Register*, Vol. 84, No. 65, April 4, 2019, pp. 13158-13177; Jarret Cummings, "**Higher Ed Community Responds to Proposed Safeguards Rule Change**," *EDUCAUSE Review*, August 14, 2019. ↵
2. Please see Jarret Cummings, "**Safeguards Rule Comments Deadline Extended to August 2**," *EDUCAUSE Review*, June 7, 2019, for more details. ↵

3. Federal Trade Commission, **"FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches,"** [↗](#) October 27, 2021. [↩](#)
4. For details, see Jarret Cummings, **"Safeguards Rule Comments Deadline Extended to August 2,"** *EDUCAUSE Review*, June 7, 2019, and Jarret Cummings, **"Higher Ed Community Responds to Proposed Safeguards Rule Change,"** *EDUCAUSE Review*, August 14, 2019. [↩](#)
5. Federal Trade Commission, **"16 CFR Part 314: Standards for Safeguarding Customer Information (Final Rule),"** [↗](#) pre-publication copy, (December 8, 2021): 5. [↩](#)
6. American Council on Education et al., letter to the Federal Trade Commission, **"Request for Public Comment on Notice of Proposed Rule-Making, 'Standards for Safeguarding Customer Information' (Safeguards Rule, 16 CFR 314, Project No. P145407),"** August 2, 2019, 3. [↩](#)
7. FTC, **"16 CFR Part 314: Standards for Safeguarding Customer Information (Final Rule),"** [↗](#) 5. [↩](#)
8. American Council on Education et al., letter to the FTC, **"Request for Public Comment on Notice of Proposed Rule-Making,** 3. [↩](#)
9. **"Record Keeping, Privacy, and Electronic Processes,"** [↗](#) in *2021-2022 Federal Student Aid Handbook in PDF Format,* [↗](#) (Washington DC: Office of Federal Student Aid, US Department of Education, 2021), 2-218, 2-220. [↩](#)

10. Jarret Cummings, "**The Safeguards Rule Audit Objective Is Here!**" *EDUCAUSE Review*, July 11, 2019. [↩](#)
 11. Federal Trade Commission, "**16 CFR Part 314: Standards for Safeguarding Customer Information (Supplemental Notice of Proposed Rulemaking)**," [↗](#) pre-publication copy, (December 8, 2021). [↩](#)
-

Jarret Cummings is Senior Policy Advisor at EDUCAUSE.

© 2021 Jarret Cummings. The text of this work is licensed under a [Creative Commons BY-NC-ND 4.0 International License](#). [↗](#)

▣ **Compliance, Cybersecurity Policy, Data Security, Encryption, Federal Student Aid, Higher Education Policy, Policy and Law**

Why IT Matters to Higher Education

EDUCAUSE
REVIEW

Higher Ed Responds to Proposed Safeguards Rule Reporting Requirement

Jarret Cummings Thursday, March 3, 2022 Policy

5 min read

The Federal Trade Commission (FTC) has proposed adding a reporting requirement to its Safeguards Rule. EDUCAUSE and its partners recommend that the FTC adopt a few revisions (e.g., delaying the public release of any Safeguards Rule security event report for one year from the submission date).

The Federal Trade Commission (FTC) published its long-awaited revisions to the Safeguards Rule in early December 2021 while giving covered entities, such as colleges and

universities, until December 2022 to achieve compliance with the many new provisions of the Rule.¹ At the same time, the FTC also proposed a new Safeguards Rule reporting requirement. Comments on the proposal were due by February 7.²

EDUCAUSE worked with member representatives to analyze the FTC's proposed provision. Our findings formed the basis of public comments jointly submitted to the FTC by the American Council on Education (ACE), EDUCAUSE, and several other groups.³ We determined that, in general, the proposal from the FTC strikes a reasonable balance between meeting its needs as a regulator and minimizing the reporting burden on institutions. A covered entity would only be required to report security events for which it has determined a misuse of customer information (primarily student financial aid information in the case of higher education) involving one thousand or more consumers has occurred or is reasonably likely to occur. Also, the entity would only have to report a few general elements:

- The name of and contact information for the organization
- A description of the types of information involved
- The date or date range of the event (if identified)
- A general description of the event itself

While the proposed reporting standard and structure would be workable overall, the FTC raised several questions indicating that it could conceivably take the final version of the regulation in some problematic directions from the higher education

perspective. With that in mind, EDUCAUSE and its partner associations provided a few specific points for the FTC to consider, with the goal of keeping the final provision largely within the initial parameters identified in its rulemaking notice.

The FTC clearly indicates in its rulemaking proposal that it wants to make the reports it would receive as a result of the new reporting provision publicly available, and it specifically asks if it should do so. The response from higher education associations argues that the information submitted under the proposed requirement would suit the needs of the FTC as a regulator that is trying to identify where it may need to work with a covered entity on possible compliance issues. It would be too high level, though, to provide meaningful information to students, parents, and other stakeholders and could conceivably raise anxiety among individual members of the campus community about whether their personal information might be involved. Given the likelihood that the public availability of the reports could generate undue concern among institutional stakeholders, EDUCAUSE and its partners suggested that posting all submitted reports to a national, publicly available web page might be counterproductive. If the FTC decides to proceed with such a plan, however, we asked it to consider delaying the public release of any Safeguards Rule security event report for one year from the date of submission. This would ensure that institutions have time to remediate the underlying event fully and communicate with all *affected* stakeholders before the general public release of the report in question.

The FTC also asked if the proposed requirement should explicitly exclude events involving encrypted information from

reporting, which would be consistent with the New York state regulations from which the overall revisions to the Safeguards Rule were drawn. The higher education groups noted that the reporting standard for the new requirement would generally lead to that result regardless, given that institutions would not consider encrypted data subject to misuse or likely misuse in the absence of some reasonable indication of the encryption having been compromised. Thus, we recommended that the FTC clearly state in the final regulation that entities are not required to report events involving encrypted information so long as no reasonable basis exists for thinking that the encryption involved is or is likely to be compromised.

Another key point that we raised concerns whether a covered entity should be allowed to delay reporting to the FTC if a law enforcement agency requests that it not share information about an event unless or until law enforcement gives its approval to do so. EDUCAUSE and its partner associations argued that if enacted, a Safeguards Rule reporting requirement should allow a covered entity to respect the wishes of law enforcement agencies and delay reporting at their request, given the general importance to cybersecurity of identifying and prosecuting bad actors to the extent possible. We noted, however, that the FTC could provide a way via its reporting process for a covered entity to inform the FTC that the entity is subject to such a request and provide contact information for the law enforcement agency or agencies in question. This would allow the FTC to negotiate with law enforcement as necessary about the conditions under which an entity could fulfill its normal reporting responsibilities sooner rather than later if the FTC thought a particular case warranted it.

Given the track record of the FTC concerning its rulemaking leading to the recently revised Safeguards Rule, EDUCAUSE members should assume that the FTC will adopt a Safeguards Rule reporting requirement that is similar to its proposed regulation. It is also highly likely that reports submitted under the new provision will become publicly available, although EDUCAUSE and its partners remain hopeful that the FTC will adopt a delay in providing public access to security event reports as we requested. The proposed Rule indicates that the FTC's final regulation will likely defer compliance for six months from the date of its official publication. With the early December compliance deadline for the new requirements, the FTC could issue the final version of its reporting provision in time for it to take effect at roughly the same time as the overall set of new Safeguards Rule mandates. Whether the FTC can achieve such a goal remains to be seen, but EDUCAUSE will continue to update members on any new developments with the proposed Safeguards Rule reporting requirement as they become available.

Notes

1. Jarret Cummings, "**Policy Analysis: Revised, Highly Prescriptive FTC Safeguards Rule,**" *EDUCAUSE Review*, December 2, 2021. ↩
2. Jarret Cummings, "**Cyber Incident Reporting Under the Safeguards Rule?**" *EDUCAUSE Review*, December 8, 2021. ↩
3. American Council on Education, et al., letter to the Federal Trade Commission, "**Request for Public Comment on Supplemental Notice of Proposed**

Rulemaking, 'Standards for Safeguarding Customer Information' (Safeguards Rule, 16 CFR 314, Project No. P145407), December 9, 2021—Proposed Security Event Reporting Requirement," February 7, 2021. ↩

Jarret Cummings is Senior Policy Advisor at EDUCAUSE.

© 2022 Jarret Cummings. The text of this work is licensed under a **Creative Commons BY-NC-ND 4.0 International License.** ↗

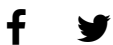
▣ **Compliance, Data Privacy, Federal Student Aid**



PUBLICATIONS


SP 800-171 Rev. 2

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

[Documentation](#)[Topics](#)

Date Published: February 2020 (includes updates as of January 28, 2021)

Supersedes: [SP 800-171 Rev. 2 \(02/21/2020\)](#).

Planning Note (4/13/2022): 

The security requirements in SP 800-171 Revision 2 are available in multiple data formats. The [PDF](#) of SP 800-171 Revision 2 is the authoritative source of the CUI security requirements. If there are any discrepancies noted in the content between the [CSV](#), [XLSX](#), and the SP 800-171 [PDF](#), please contact sec-cert@nist.gov and refer to the PDF as the normative source.

CUI SSP template

** There is no prescribed format or specified level of detail for system security plans. However, organizations ensure that the required information in [SP 800-171 Requirement] 3.12.4 is conveyed in those plans.

Author(s)

Ron Ross (NIST), Victoria Pillitteri (NIST), Kelley Dempsey (NIST), Mark Riddle (NARA), Gary Guissanie (IDA)

Abstract

The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully conduct its essential missions and functions. This publication... [See full abstract](#)

Keywords


basic security requirement; contractor systems; Controlled Unclassified Information; CUI Registry; derived security requirement; Executive Order 13556; FIPS Publication 199; FIPS Publication 200; FISMA; NIST Special Publication 800-53; nonfederal systems; security assessment; security control; security requirement; nonfederal organizations

Control Families

Access Control; Audit and Accountability; Awareness and Training; Configuration Management; Identification and Authentication; Maintenance; Media Protection; Personnel Security; Physical and Environmental Protection; System and Communications Protection; System and Information Integrity

DOCUMENTATION

Publication:

 [SP 800-171 Rev. 2 \(DOI\)](#)

 [Local Download](#)

Supplemental Material:

 [Security Requirements Spreadsheet \(xls\)](#)

 [Security Requirements CSV \(other\)](#)

 [README for CSV \(txt\)](#)

 [CUI Plan of Action template \(word\)](#)

 [CUI SSP template ^{**}\[see Planning Note\] \(word\)](#)

 [Mapping: Cybersecurity Framework v.1.0 to SP 800-171 Rev. 2 \(xls\)](#)

Other Parts of this Publication:

[SP 800-171A](#)

Related NIST Publications:

[SP 800-172](#)

Document History:

01/28/21: SP 800-171 Rev. 2 (Final)

TOPICS

Security and Privacy

[audit & accountability](#); [awareness training & education](#); [maintenance](#); [security controls](#); [threats](#)

Laws and Regulations

Federal Acquisition Regulation; Federal Information Security Modernization Act

HEADQUARTERS

100 Bureau Drive
Gaithersburg, MD 20899



Want updates about CSRC and our publications?

Subscribe

[Webmaster](#) | [Contact Us](#) | [Our Other Offices](#)

Contact CSRC Webmaster: webmaster-csrc@nist.gov

[Site Privacy](#) | [Accessibility](#) | [Privacy Program](#) | [Copyrights](#) | [Vulnerability Disclosure](#) |

[No Fear Act Policy](#) | [FOIA](#) | [Environmental Policy](#) | [Scientific Integrity](#) |

[Information Quality Standards](#) | [Commerce.gov](#) | [Science.gov](#) | [USA.gov](#) | [Vote.gov](#)

Resource**Center** (/resources)

All the privacy tools and information you need in one easy-to-find place

in (<https://www.linkedin.com/company/iapp---international-association-of-privacy-professionals/>) **🐦**

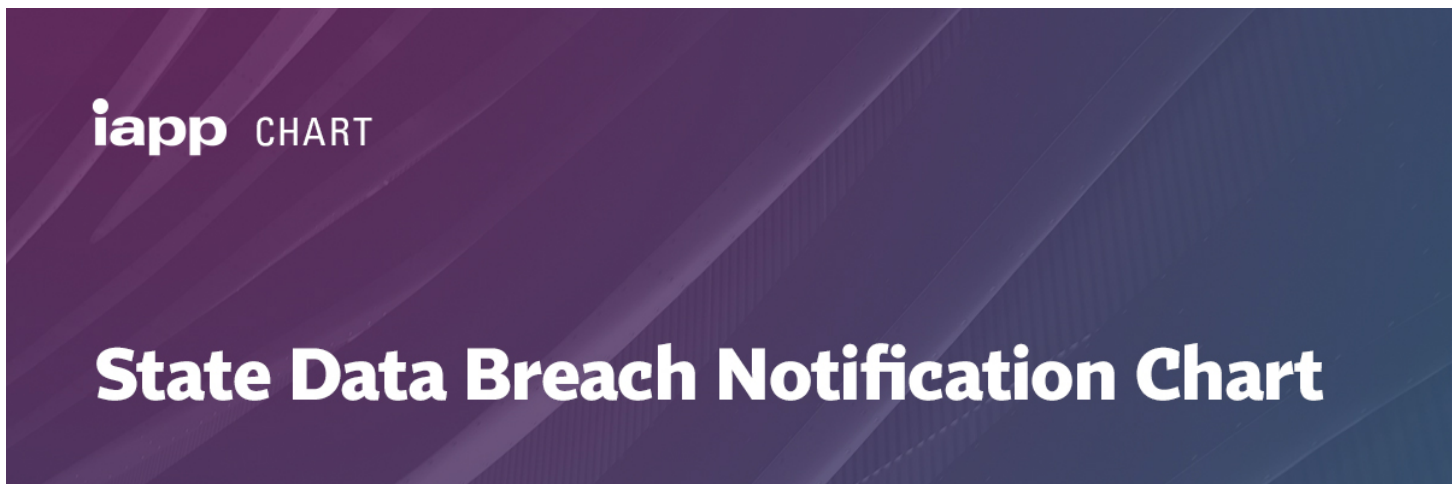
(<https://twitter.com/PrivacyPros>) **@** (<https://www.instagram.com/iappprivacypros/?hl=en>) **f**

(<https://www.facebook.com/IAPPprivacypros>) **▶** (<https://www.youtube.com/user/IAPPvideos>)

+ [Save This \(\)](#)

State Data Breach Notification Chart

Cheryl Saniuk-Heinig, CIPP/US (<https://iapp.org/about/person/0011a00000vzaVGAAAY>)



(https://iapp.org/media/resource_center/iapp__us_state_data_breach_notification_chart.xlsx)

Last Updated: March 2021

[Click To View \(XLSX\)](https://iapp.org/media/resource_center/iapp__us_state_data_breach_notification_chart.xlsx)
(https://iapp.org/media/resource_center/iapp__us_state_data_breach_notification_chart.xlsx)

U.S. data breach notification laws vary across all 50 states and U.S. territories. Each law must be applied to every factual scenario to determine if a notification requirement is triggered.

territory's data breach notification law concerning entities that own, control or process personal data. The main sheet of this chart, titled "All Data – Alphabetical," lists all states followed by U.S. territories and contains:

- A hyperlink to the state's notification statute.
- The timeframe in which notification to impacted individuals is required.
- Any exceptions to notification requirements.
- If and when notification must be made to a state agency, consumer protection agency or consumer reporting agency.
- Special forms or language that must be included in the notice.
- Whether the statute provides for a private right of action.

Each column can be filtered to allow notification laws with certain features to be hidden or prioritized. As a starting point, a practitioner could filter the "Timeframe for Breach Notification" column to identify which states have the shortest notification window to further investigate the state-specific requirements. For convenience, the IAPP has also included subsequent sheets with three categories of pre-sorted data:

- Shortest notification timeframe.
- Requires attorney general notification (ranked from the lowest number of impacted individuals to highest).
- Requires consumer reporting agency notification (ranked from the lowest number of impacted individuals to highest).

This chart does not include exceptions to or additional compliance requirements with federal laws, such as the Gramm-Leach-Bliley Act or the Health Insurance Portability and Accountability Act. Additionally, an entity must determine if it owns, controls or licenses "personally identifiable information" before it can determine if the "personally identifiable information" was compromised in a "breach" (compared to a security "event" or "incident"), which will be uniquely defined by each law.

NOTE: This tool is for informational purposes only and is not legal advice. State requirements, including any recent changes, should always be verified via official sources. Requirements, if there is a security event, incident or breach, will vary depending on the

Tags: [Data Loss \(/tag/data-loss\)](#), [Infosecurity \(/tag/infosecurity\)](#), [Privacy Law \(/tag/privacy-law\)](#), [Privacy Operations Management \(/tag/privacy-operations-management\)](#), [Privacy Research \(/tag/privacy-research\)](#)

© 2022 International Association of Privacy Professionals.
All rights reserved.

Pease International Tradeport, 75 Rochester Ave.
Portsmouth, NH 03801 USA • +1 603.427.9200



visitors, customers, and employees during the COVID-19 (coronavirus) pandemic. NARA's facilities are closed until further notice and in-person services for the public and other Federal agencies have been suspended almost entirely. All ISOO staff are teleworking remotely and we are making every effort to continue providing services whenever possible, using online and remote capabilities. ISOO's ability to serve our customers in a timely manner may be hampered by the current crisis. To ensure a more timely response to your inquiry, please contact us via email at [isoo@nara.gov / cui@nara.gov / iscap@nara.gov] We ask for your understanding and appreciate your patience. ISOO will use its blog, ISOO Overview to communicate with stakeholders on all ISOO matters. Please join for weekly posts.

Please visit the CUI blog: Controlled Unclassified Information for more information.


Established by Executive Order 13556, the Controlled Unclassified Information (CUI) program standardizes the way the Executive branch handles unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies. [Learn About CUI](#)

CUI Registry

The CUI Registry is the Government-wide online repository for Federal-level guidance regarding CUI policy and practice. However, agency personnel and contractors should first consult their agency's CUI implementing policies and program management for guidance.

Search the Registry:

Categories, Markings and Controls:

- [Category List](#)
- [CUI Markings](#)
- [Limited Dissemination Controls](#)
- [Decontrol](#)
- [Registry Change Log](#) 

Policy and Guidance

- [Executive Order 13556](#)
- [32 CFR Part 2002 \(Implementing Directive\)](#)
- [CUI Marking Handbook](#)
- [CUI Notices](#)

CUI Glossary



CUI Training

Learn about training tools developed by the Executive Agent for CUI users.



Oversight

Learn about CUI oversight requirements and tools.



CUI Resources

Learn about additional tools for handling CUI, including:

- CUI Coversheet
- CUI Marking Trifold Brochure
- CUI Audio/Photo/Video Markings Brochure
- CUI Destruction Label
- CUI Email Marking Tip
- CUI Media Labels

The U.S. National Archives and Records Administration

1-86-NARA-NARA or 1-866-272-6272



CUI Category: Student Records

Banner Marking for Specified Authorities: CUI//SP-STUD

Banner Marking for Basic Authorities: CUI

Category Description:	As per 20 USC 1232g, the Family Educational Rights and Privacy Act of 1974, an education record which is comprised of those records which are directly related to a student.
Category Marking:	STUD
Alternative Banner Marking for Basic Authorities:	CUI//STUD

<p>Banner Format and Marking Notes:</p>	<p>Banner Format: CUI//Category Marking//Limited Dissemination Control</p> <p>Marking Notes:</p> <ul style="list-style-type: none"> • The CUI Control Marking may consist of either the word “CONTROLLED” or the acronym “CUI”, depending on agency policy. • Category marking is optional when marking Basic CUI unless required by agency policy. Example: CUI//Limited Dissemination Control. • Category Marking preceded by "SP-" is required when marking Specified CUI. Example: CUI//SP-Category Marking//Limited Dissemination Control • Whether CUI is Basic or Specified is determined by the applicable Safeguarding and/or Dissemination Authority for a given instance of CUI. • Separate multiple Category Markings by a single forward slash (/) and list Category Markings alphabetically. Example: CUI//Category Marking A/Category Marking B//Limited Dissemination Control • Category Markings for Specified CUI precede Category Markings for Basic CUI. Example: CUI//SP-Category Marking/Category Marking//Limited Dissemination Control • Separate multiple Limited Dissemination Controls by a single forward slash (/). Example: CUI//Category Marking//Limited Dissemination Control/Limited Dissemination Control • Reference 32 CFR 2002.20 , CUI Marking Handbook , Limited Dissemination Controls and individual agency policy for additional and specific marking guidelines
--	---

Notes for Safeguarding, Dissemination and Sanction Authorities:

- Whether CUI is Basic or Specified is determined by the applicable Safeguarding and/or Dissemination Authority for that CUI.
- Each "Safeguarding and/or Dissemination Authority" citation links to the statute, regulation or government-wide policy authorizing the control of that information as CUI.
- Each "Sanctions" authority links to the statute, regulation or government-wide policy that includes penalties for CUI misuse of CUI for the associated "Safeguarding and/or

Dissemination Authority" on the same line.

Safeguarding and/or Dissemination Authority	Basic or Specified	Banner Marking	Sanctions
20 USC 1232g(a)(1)(C)	Basic	CUI	
25 CFR 43.14	Basic	CUI	
25 CFR 43.22	Specified	CUI//SP-STUD	
34 CFR 99.30(a)	Basic	CUI	
34 CFR 99.31(a)(6)(ii)	Basic	CUI	
34 CFR 99.33(a)(1)	Basic	CUI	

Authority links are updated based on regular re-publication of the United States Code and Code of Federal Regulations, and the CUI Registry maintenance schedule.

The U.S. National Archives and Records Administration

1-86-NARA-NARA or 1-866-272-6272

Federal Student Aid

An OFFICE of the U.S. DEPARTMENT of EDUCATION

Published on <https://fsapartners.ed.gov/knowledge-center/library/electronic-announcements/2020-12-18/protecting-student-information-compliance-cui-and-glba>

POSTED DATE: December 18, 2020

AUTHOR: Federal Student Aid

SUBJECT: Protecting Student Information – Compliance with CUI and GLBA

As instances of data and information breaches rise, it is vital that institutions of higher education (IHEs) protect Controlled Unclassified Information (CUI) used in the administration of federal student aid programs authorized under Title IV, of the Higher Education Act, as amended¹. FSA is finalizing the Campus Cybersecurity Program framework. A multi-year phased implementation will begin with a self-assessment of the National Institute of Standards and Technology Special Publication 800–171 Rev. 2, *Controlled Unclassified Information in Nonfederal Systems* (NIST 800–171 Rev. 2) readiness and outreach activities. We are committed to fully advancing and encouraging all postsecondary institutions implementation of NIST 800-171 controls.

This Electronic Announcement is meant to inform IHEs and their third-party servicers about upcoming activities to ensure compliance with NIST 800–171 Rev. 2. Institutions' compliance is in accordance with 32 C.F.R. Part 2002 and the federal government-wide requirement that institutions receiving CUI from the U.S. Department of Education (Department) comply with NIST 800–171 Rev. 2². FSA has previously encouraged IHEs to review and adopt NIST 800–171 Rev. 2 as a security standard and to support continuing obligations under the Gramm-Leach-Bliley Act (GLBA). Since 2018, many institutions have adopted some or all of the NIST 800–171 recommended requirements. We further encourage use of NIST 800–171 Rev. 2 to help mitigate risks related to CUI.

In 2021, FSA plans to initiate a self-assessment effort to understand the IHE community's readiness to comply with NIST 800–171 Rev 2. The self-assessment effort will help the Department determine the cybersecurity posture, maturity, and future compliance of each IHE with NIST 800–171 and other cybersecurity requirements. Our intention is to partner and collaborate with IHEs, and other organizations, to enhance the resilience and maturity across IHEs by establishing a cybersecurity baseline, sharing information, and overseeing compliance with NIST 800–171 Rev. 2 and other cybersecurity requirements.

Instances of data breaches at organizations entrusted with personally identifiable information (PII) continue to proliferate and reinforce the need for the Department and IHEs to work together to combat cybersecurity threats and strengthen cybersecurity infrastructure at IHEs. Ensuring the confidentiality, security, and integrity of Title IV information depends on cooperation between the Department, IHEs, and other entities, including state grant agencies, lenders, contractors, and third-party servicers.

We expect federal student aid partners to develop, implement, and enhance information security programs with requisite controls and monitoring that supports all aspects of the administration of Title IV federal student aid programs. These security programs must encompass all systems, databases, and processes that collect, process, and distribute information — including PII — in support of applications for and receipt of Title IV student assistance.

Protecting Student Information – Next Steps

The Department looks forward to continued collaboration with IHEs to protect student data. We are committed to supporting IHEs and are working to provide additional guidelines and best practices to implement the government-wide CUI requirements, leveraging NIST security guidance. In 2021, we will post additional information to provide further information and guidance, including the cybersecurity self-assessment. In the meantime, institutions are strongly encouraged to learn more about NIST 800–171 Rev. 2 and sharing with your IT team to reduce risk surrounding CUI.

Background

The Student Aid Internet Gateway (SAIG) Enrollment Agreement entered into by each Title IV-participating institution includes a provision that the institution “[m]ust ensure that all Federal Student Aid applicant information is protected from access by or disclosure to unauthorized personnel.” Institutions are reminded that under various federal and state laws and other authorities — including the HEA;³ the *Family Educational Rights and Privacy Act* (FERPA); the *Privacy Act of 1974*, as amended; the GLBA; and state data breach and privacy laws — institutions may be responsible for losses, fines, and penalties (including criminal penalties) as a result of data breaches.


CUI is government-created or -owned information that requires safeguarding or dissemination controls consistent with applicable laws, regulations, and government-wide policies. National Archives and Records Administration's CUI rule, effective Nov. 14, 2016, 32 C.F.R. Part 2002.16, establishes that agencies must enter into an agreement with a non-executive branch entity to share CUI and require compliance with the standards set forth in the NIST 800-171 Rev. 2. The CUI program standardizes the way the Executive branch agencies handles unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and federal government-wide policies. Most data sourced from the Department and information used in the administration of Title IV programs are considered CUI.

Contact Information

If you have questions about compliance with CUI and GLBA, please contact the Cybersecurity Team at FSA_IHECyberCompliance@ed.gov or by phone at 202-245-6550.

References:

[National Institute of Standards and Technology Special Publication 800-171 Rev 2 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations](#) 

[National Institute of Standards and Technology Special Publication 800-172 Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171 \(Final Public Draft\)](#) 

[Federal Trade Commission Safeguards Rule](#) 

¹ 20 U.S.C. § 1070, et seq.

² 32 CFR § 2002.16 (5) (“Agencies should enter into agreements with any non-executive branch or foreign entity with which the agency shares or intends to share CUI.”).

³ See 20 U.S. Code § 1018b (“Any entity that maintains or transmits information under a transaction covered by this section shall maintain reasonable and appropriate administrative, technical, and physical safeguards.”).

<https://www.nist.gov/blogs/manufacturing-innovation-blog/what-nist-sp-800-171-and-who-needs-follow-it-0>



Manufacturing Innovation Blog

(<https://www.nist.gov/blogs/manufacturing-innovation-blog>)

Powered by the [Manufacturing Extension Partnership](https://www.nist.gov/mep) (<https://www.nist.gov/mep>)

What Is the NIST SP 800-171 and Who Needs to Follow It?

October 8, 2019

By: [Traci Spencer](https://www.nist.gov/blogs/manufacturing-innovation-blog/authors/traci-spencer) (<https://www.nist.gov/blogs/manufacturing-innovation-blog/authors/traci-spencer>)



This article originally appeared on [IndustryWeek](https://www.industryweek.com/sponsored/what-nist-sp-800-171-cybersecurity-framework)

(<https://www.industryweek.com/sponsored/what-nist-sp-800-171-cybersecurity-framework>).

Guest blog post by Traci Spencer, Grant Program Manager for TechSolve, Inc., the southwest regional partner of the Ohio MEP, part of the MEP National NetworkTM.

Manufacturers involved in supply chains tied to government contracts can anticipate those awards bringing in additional revenue at levels that might not be possible otherwise. However, being successful in getting and keeping such work means

complying with the Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS).

FAR is a set of regulations that governs all acquisitions and contracting procedures associated with the U.S. government. DFARS accompanies FAR as an addition. The Department of Defense (DoD) is the administrative body behind DFARS, but the reach of DFARS requirements extends to more than that organization.

NIST SP 800-171 is a NIST Special Publication that provides recommended requirements for protecting the confidentiality of controlled unclassified information (CUI). Defense contractors must implement the recommended requirements contained in NIST SP 800-171 to demonstrate their provision of adequate security to protect the covered defense information included in their defense contracts, as required by DFARS clause 252.204-7012. If a manufacturer is part of a DoD, General Services Administration (GSA), NASA or other federal or state agencies' supply chain, the implementation of the security requirements included in NIST SP 800-171 is a must.

How Do You Implement NIST SP 800-171?

It's understandable for manufacturers to wonder what they should do to implement NIST SP 800-171 and ultimately get in compliance with DFARS, and whether there are specialized resources available to help them achieve that milestone without preventable pitfalls. The first thing they should keep in mind is that being DFARS compliant likely involves working with a cybersecurity consultant that knows the NIST SP 800-171 requirements inside and out.

It's advisable for small manufacturers to look to their state's Manufacturing Extension Partnership (MEP) Center. Part of the MEP National Network™, a larger organization that connects them to NIST, the representatives at your local MEP Center will have a working knowledge of NIST SP 800-171 and can help companies prepare for DFARS compliance. It can be a short or long process, depending upon the complexities of a company's operating environment and information systems, but implementing NIST SP 800-171 is a necessary process for a company to protect its information.

What Does a Successful Plan Entail?

Manufacturers that want to retain their DoD, GSA, NASA and other federal and state agency contracts need to have a plan that meets the requirements of NIST SP 800-171. DFARS cybersecurity clause 252,204-7012 went into effect on Dec. 31, 2017, and deals

with processing, storing or transmitting CUI that exists on non-federal systems — such as those used by a government contractor.

One of the first steps manufacturers should take is to identify where gaps exist that prevent them from being compliant with DFARS. From that point, they can determine how to proceed.

How Should Manufacturers Start Working Toward Compliance?

The MEP National Network offers dedicated resources for manufacturers (<https://www.nist.gov/mep/cybersecurity-resources-manufacturers>) that need information about a company's cybersecurity posture that can help companies understand what getting compliant with DFARS actually means to them. Companies can see whether DFARS compliance applies to them and view infographics that recommend steps to take to make their factory floors more secure.

The MEP National Network also provides a particular resource that manufacturers will undoubtedly refer to again and again: the NIST Self-Assessment Handbook (<https://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf>) (NIST Handbook 162) (<https://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf>). It spans more than 150 pages and helps readers assess their facilities to conclude how close they are to implementing NIST SP 800-171 to help them understand how close they are to being DFARS compliant. It also helps determine where to focus efforts when making improvements to maximize the impact of each dollar spent on cybersecurity.

For example, the document features content that advises how to go about carrying out an assessment and which applicable employees to talk to regarding security requirements. Manufacturers that read through the handbook will note that each assessment question has an "alternative approach" option. It refers to the fact that manufacturers may find some requirements in NIST SP 800-171 that don't apply to them.

In that case, it's acceptable to use a different but equally effective method of maintaining security — as long as the respective manufacturers notify the correct government authorities about the changes and get approval for them.

Manufacturing plant representatives can also increase their understanding of compliance requirements by watching a webinar (<https://bluejeans.com/playback/s/VZevy5gUYLnIO2QOEXrt3GVCoAJp1cWKmK21oR6S1DVGcCtYmftQ05DG7zNVVm46>) that goes through some of the crucial elements of the handbook.

Complexity Shouldn't Be a Barrier

Manufacturers may initially view the cybersecurity requirements for government contracts as too complicated, especially if they have small operations.

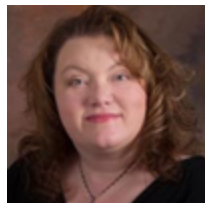
However, using the available resources — including local MEP Centers — allows manufacturers to realize it's possible to get in compliance with DFARS, as well as stay in compliance, by implementing the NIST SP 800-171 requirements and to open possibilities for receiving financially rewarding and reputation-boosting government contracts.

A local MEP Center is an ideal resource for manufacturers to use as they start to complete a plan that details how to implement the NIST SP 800-171 cybersecurity requirements.

Each MEP Center has access to public and private sector resources that can help companies get into compliance with more confidence. Locations exist in [all 50 states and Puerto Rico](https://www.nist.gov/mep/mep-national-network/connect-your-local-mep-center) (<https://www.nist.gov/mep/mep-national-network/connect-your-local-mep-center>).

[Cybersecurity](https://www.nist.gov/manufacturing-innovation-blog-categories/cybersecurity) (<https://www.nist.gov/manufacturing-innovation-blog-categories/cybersecurity>).

About the author



Traci Spencer (<https://www.nist.gov/blogs/manufacturing-innovation-blog/authors/traci-spencer>)

Traci Spencer is the Grant Program Manager for TechSolve, Inc., the southwest regional partner of the Ohio MEP. A member of the MEP National Network Cybersecurity Working Group, she recently completed...

Related posts



[Cybersecurity for the Manufacturing Sector: Reduce Data Integrity Breaches with NIST SP 1800-10](https://www.nist.gov/blogs/manufacturing-innovation-blog/cybersecurity-manufacturing-sector-reduce-data-integrity) (<https://www.nist.gov/blogs/manufacturing-innovation-blog/cybersecurity-manufacturing-sector-reduce-data-integrity>)

[blog/cybersecurity-manufacturing-sector-reduce-data-integrity](https://www.nist.gov/blogs/manufacturing-innovation-blog/cybersecurity-manufacturing-sector-reduce-data-integrity))

April 21, 2022

Industrial control systems (ICS) help manufacturers boost productivity, optimize efficiency and advance production lines. Historically, ICS networks were



Supporting Digital Transformation with Legacy Components (<https://www.nist.gov/blogs/manufacturing-innovation-blog/supporting-digital-transformation-legacy-components>)

July 20, 2021

“Information is the oil of the 21st century, and analytics is the combustion engine.” – Peter Sondergaard, Senior Vice President, Gartner Research Digital



Commonly Misused Terms in Cybersecurity

(<https://www.nist.gov/blogs/manufacturing-innovation-blog/commonly-misused-terms-cybersecurity>)

June 25, 2021

Words are hard. English is hard. How we manage to communicate anything is nigh a miracle. Sometimes I wish I was Oscar Wilde or Mark Twain or any of the other

About this blog

Manufacturing Innovation, the blog of the [Manufacturing Extension Partnership \(MEP\)](https://www.nist.gov/mep) (<https://www.nist.gov/mep>), is a resource for manufacturers, industry experts and the public on key U.S. manufacturing topics. There are articles for those looking to dive into new strategies emerging in manufacturing as well as useful information on tools and opportunities for manufacturers.

The views presented here are those of the author and do not necessarily represent the views or policies of NIST.

If you have any questions about our blog, please contact us at mfg@nist.gov (<https://www.nist.gov/mailto:mfg@nist.gov>).

ABOUT CMMC

Frequently Asked Questions

✓ [NOW THAT CMMC 2.0 IS PUBLISHED, WILL COMPANIES BE REQUIRED TO COMPLY WITH CMMC 1.0?](#)

✓ [WHEN WILL CMMC 2.0 BE REQUIRED FOR DOD CONTRACTS?](#)

✓ [WHY DID THE DEPARTMENT MAKE THESE CHANGES?](#)

✓ [HOW MUCH WILL IT COST TO IMPLEMENT CMMC 2.0?](#)

CMMC 2.0 Briefing

- [Briefing Overview](#) (03 DEC 2021)

Current DoD Cybersecurity Efforts

- [Link to Document](#) (07 DEC 2021)

Cybersecurity is a top priority for the Department of Defense.

The Defense Industrial Base (DIB) is the target of increasingly frequent and complex cyberattacks. To protect American ingenuity and national security information, the DoD developed CMMC 2.0 to dynamically enhance DIB cybersecurity to meet evolving threats and safeguard the information that supports and enables our warfighters.

OVERVIEW OF THE CMMC PROGRAM

The Cybersecurity Maturity Model Certification (CMMC) program enhances cyber protection standards for companies in the DIB. It is designed to protect sensitive unclassified information that is shared by the Department with its contractors and subcontractors. The program incorporates a set of cybersecurity requirements into acquisition programs and provides the Department increased assurance that contractors and subcontractors are meeting these requirements.

The framework has three key features:

- **Tiered Model:** CMMC requires that companies entrusted with national security information implement cybersecurity standards at progressively advanced levels, depending on the type and sensitivity of the information. The program also sets forward the process for information flow down to subcontractors.
- **Assessment Requirement:** CMMC assessments allow the Department to verify the implementation of clear cybersecurity standards.
- **Implementation through Contracts:** Once CMMC is fully implemented, certain DoD contractors that handle sensitive unclassified DoD information will be required to achieve a particular CMMC level as a condition of contract award.

THE EVOLUTION TO CMMC 2.0

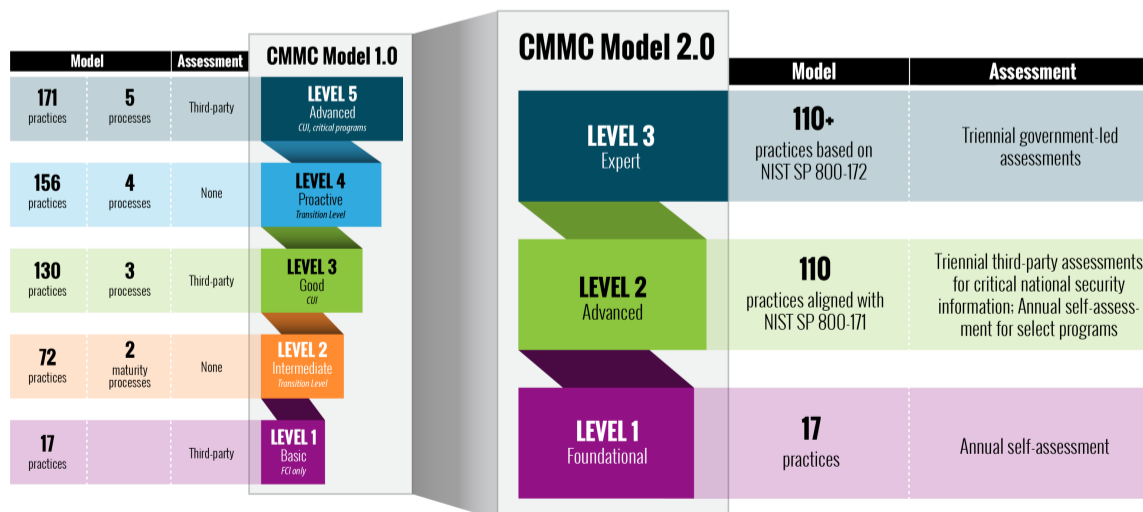
In September 2020, the DoD published an interim rule to the DFARS in the Federal Register (DFARS Case 2019-D041), which implemented the DoD’s initial vision for the CMMC program (“CMMC 1.0”) and outlined the basic features of the framework (tiered model, required assessments, and implementation through contracts). The interim rule became effective on November 30, 2020, establishing a five-year phase-in period.

In March 2021, the Department initiated an internal review of CMMC’s implementation, informed by more than 850 public comments in response to the interim DFARS rule. This comprehensive, programmatic assessment engaged cybersecurity and acquisition leaders within DoD to refine policy and program implementation.

In November 2021, the Department announced “CMMC 2.0,” an updated program structure and requirements designed to achieve the primary goals of the internal review:

- Safeguard sensitive information to enable and protect the warfighter
- Dynamically enhance DIB cybersecurity to meet evolving threats
- Ensure accountability while minimizing barriers to compliance with DoD requirements
- Contribute towards instilling a collaborative culture of cybersecurity and cyber resilience
- Maintain public trust through high professional and ethical standards

KEY FEATURES OF CMMC 2.0



With the implementation of CMMC 2.0, the Department is introducing several key changes that build on and refine the original program requirements. These are:



Streamlined Model

- **Focused on the most critical requirements:** Streamlines the model from 5 to 3 compliance levels
- **Aligned with widely accepted standards:** Uses National Institute of Standards and Technology (NIST) cybersecurity standards



Reliable Assessments

- **Reduced assessment costs:** Allows all companies at Level 1 (Foundational), and a subset of companies at Level 2 (Advanced) to demonstrate compliance through self-assessments
- **Higher accountability:** Increases oversight of professional and ethical standards of third-party assessors



Flexible Implementation

- **Spirit of collaboration:** Allows companies, under certain limited circumstances, to make Plans of Action & Milestones (POA&Ms) to achieve certification
- **Added flexibility and speed:** Allows waivers to CMMC requirements under certain limited circumstances

RULEMAKING AND TIMELINE FOR CMMC 2.0

The changes reflected in CMMC 2.0 will be implemented through the rulemaking process. Companies will be required to comply once the forthcoming rules go into effect. The Department intends to pursue rulemaking both in Part 32 of the Code of Federal Regulations (C.F.R.) as well as in the Defense Federal Acquisition Regulation Supplement (DFARS) in Part 48 of the C.F.R. Both rules will have a public comment period. Stakeholder input is critical to meeting the objectives

of the CMMC program, and the Department will actively seek opportunities to engage stakeholders as it drives towards full implementation.

While these rulemaking efforts are ongoing, the Department intends to suspend the current CMMC Piloting efforts and will not approve inclusion of a CMMC requirement in any DoD solicitation.

The Department encourages contractors to continue to enhance their cybersecurity posture during the interim period while the rulemaking is underway. The Department has developed [Project Spectrum](#) to help DIB companies assess their cyber readiness and begin adopting sound cybersecurity practices.

The DoD is exploring opportunities to provide incentives for contractors who voluntarily obtain a CMMC certification in the interim period. Additional information will be provided as it becomes available.



CONTACT US

Please provide any questions or comments utilizing the contact form.

NAME

Please enter your name

EMAIL

Please enter your email address

SUBJECT

Technical Issue with the Website

MESSAGE

Please include a detailed message

Send Email

Acquisition & Sustainment

Army Acquisition

Office of the Assistant Secretary of Defense for Acquisition

Army Sustainment

Office of the Assistant Secretary of Defense for Sustainment

Army IE&E

Office of the Assistant Secretary of Defense for Nuclear,
Chemical, and Biological Defense Programs

Navy Acquisition

Office of the Deputy Assistant Secretary of Defense for Industrial
Policy

Navy Sustainment

Office of the Executive Director for Special Access Program
Central Office

Navy EI&E

Office of the Executive Director for International Cooperation

Air Force Acquisition

Air Force Sustainment

Air Force EI&E

Resources

[Accessibility | Section 508](#)

[Freedom of Information Act](#)

[DoD No FEAR Act](#)

[Plain Writing Act](#)

[Defense Strategic Plan](#)

[National Defense Strategy](#)

[USA.gov](#)

[Web Policy](#)

[External Link Disclaimer](#)

DoD Links

[US Department of Defense](#)

[USD Chief Management Office](#)

[USD Research & Engineering](#)

[USD Policy](#)

[USD Comptroller](#)

[USD Personnel & Readiness](#)

[USD Intelligence](#)

[DoD CIO](#)

[DoD Inspector General](#)

[Privacy & Security](#) | [Sitemap](#)

2022 Official U.S. Department of Defense Website

