# Higher Ed Student Privacy Working Group Meeting Notes

Friday, October 27, 2017
11:30am-12:30pm
Topic: Higher Ed & Security: CIPSEA & FISMA & NIST Webinar
37 Attendees

**Chris Sadler, Education Data & Privacy Fellow, New America's Open Technology Institute on Federal Information Security Management Act (FISMA) passed in 2002 as Title II of the E-Government Act.**

FISMA provides cradle to grave guidance for information security practices.

There are some gray areas regarding whether or not something constitutes a "system" under FISMA.

NIST Risk Management Framework:

1) Categorize
    - Reference FIPS 199: Standards for Security Categorization of Federal Information
        - Define Impact
        - Uses 3 different Security Dimensions
            - Confidentiality: keeping the data private
            - Integrity: ensuring the data isn't tampered with
            - Availability: how prevalent the attack might be
2) Select/Implement/Access Controls
    - Reference FIPS 200: Minimum Security requirements for federal systems
        - 17 categories of security controls
    - Reference NIST 800-53
            - Tells you which controls to apply based on how you defined the impact level
            - This process can be contracted out
3) Authorize System
    - Seek the appropriate authority to proceed
4) Continuous Monitoring
    - Look at control to make sure that they are working
        - NIST 800-137
            - Define
            - Establish
            - Implement
            - Analyze and Response
            - Review and Update
    - Continue to scan for intrusions
        - Vulnerability management
        - Patch management
        - Event and incident management

- Malware detection
- Asset, License, and Configuration Management
- Network Management
- Information Management

**Michael Hawes, U.S. Department of Education, Director of Student Privacy Policies on Title V – Confidential Information Protection and Statistical Efficiency Act of 2002 of the E-Government Act of 2002 (CIPSEA)**

Pronounce it, "Sip-See"

The purpose of CIPSEA is to reduce public confusion and uncertainty regarding the treatment of confidential statistical information the government collects. It provides strong confidentiality protections to many Federal agencies conducting statistical information collections such as surveys and censuses as well as other statistical activities including data analysis and modeling, etc. Generally speaking, most student data isn't considered statistical data when it's collection but it can depending on what's done with that data.

CIPSEA is imposed on agencies that (1) acquire information for exclusively statistical purposes under a pledge of confidentiality, or (2) they possess or access information protected by CIPSEA, unless even stronger confidentiality protections apply.

There are two subtitles under CIPSEA.

Subtitle A: Confidential Information Protection, concerns confidentiality and statistical uses of information.

The purposes of Subtitle A are:

1. to ensure that information supplied by individuals or organizations to an agency for statistical purposes under a pledge of confidentiality is used exclusively for statistical purposes;
2. to ensure that individuals or organizations who supply information under a pledge of confidentiality to agencies for statistical purposes will neither have that information disclosed in identifiable form to anyone not authorized by this title nor have that information used for any purpose other than a statistical purpose; and
3. to safeguard the confidentiality of individually identifiable information acquired under a pledge of confidentiality for statistical purposes by controlling access to, and uses made of, such information.

Subtitle B: Promotes statistical efficiency by permitting limiting

1. to authorize the sharing of business data among Census, BEA, and BLS for exclusively statistical purposes;
2. to reduce the paperwork burdens imposed on businesses that provide requested information to the Federal Government;

3. to improve the comparability and accuracy of Federal economic statistics by allowing Census, BEA, and BLS to update sample frames, develop consistent classifications of establishments and companies into industries, improve coverage, and reconcile significant differences in data produced by the three agencies; and
4. to increase understanding of the United States economy, especially for key industry and regional statistics, to develop more accurate measures of the impact of technology on productivity growth, and to enhance the reliability of the Nation's most important economic indicators, such as the National Income and Product Accounts.

So why CIPSEA? There were more than 70 federal agencies or organizational units that had statistical information for a variety of reasons. Prior to CIPSEA, there was no comprehensive way to deal with how statistical data was protected.

Benefits:

By establishing a uniform policy for all federal government statistical agency, CIPSEA stands to reduce public confusion and uncertainty about the treatment of confidential statistical information the federal government collects.

By establishing a consistent set of rational principles and processes to buttress those confidentiality pledges, the law really enables the federal government to harmonize these confidentiality claims and to set minimal standards for safeguarding any confidential statistical information.

Key Components of what CIPSEA protects is the distinction between statistical information and non statistical information.

Under CIPSEA, a ***statistical purpose*** includes the description, estimation, or analysis of the characteristics of groups, without identifying the individuals or organizations that comprise such groups, while non-statistical purposes include any administrative, regulatory, law enforcement, adjudicatory, or other purpose that affects the rights, privileges, or benefits of a particular respondent.

A ***non-statistical purpose*** means the use of data in identifiable form for any purpose that is not a statistical purpose, including any administrative, regulatory, law enforcement, adjudicatory, or other purpose that affects the rights, privileges, or benefits of a particular identifiable respondent.

Confidential information is also exempt from release under FOIA.

Penalties:
CIPSEA carries a number of strong penalties. There can be imprisonment for up to 5 years and/or a fine of up to $250,000 for whoever willfully discloses the information in any manner to a person or agency not entitled to receive it.

The implications for researchers is: well the law is mostly for federal agencies that collect statistical data. A statistical agency or unit may designate agents, by contract or by entering into

a special agreement containing the provisions required under CIPSEA. They must have written contracts and a statement that binds them to the same penalties as federal agencies for the disclosure of information. Also they must be under the direct control of the federal agency.

CIPSEA doesn't provide a right of access to statistical data for federal researchers. Individuals who want to obtain CIPSEA data will have to agree to the rules governing that data.

CIPSEA was a milestone piece of legislation for statistical agencies. It provided a single framework for the federal government to collection a statistical framework for agencies who collect statistical data for statistical purposes. It provides a backbone of strong confidentiality protections.

**Question & Answer**

Question: **How long does it typically take to go through the FISMA process from beginning to end (even just a rough time range)?**

> Answer: Rough time range, from start of categorization to getting authority to operate: 1 year. It varies, though. It's a long process of getting security controls in place and getting them tested.

Question: **Is IPEDS considered a "statistical collection" for purposes of CIPSEA?**

> Answer: IPEDS is data collection that is administered by the NCES, but the way I understand it, it's not considered a CIPSEA collection, it's considered a administrative data collection.

Question: **How does FISMA, NIST, and CIPSEA relate to the introduced College Transparency Act?**

> Answer: I'm not sure post OPM how you do all of this stuff. I don't know. These days just saying that you're going to strictly adhere to NIST standards isn't enough. We are doing something that's in line with the current policy. We're only going to store aggregate statistics and not retain the raw data. I think it's important to highlight that we're doing something a little different. We're going to emphasize that it's not a system, it's not a database...There are a lot of limitations within CTA as to what data can be collected. When it comes to CIPSEA, I think it's important that this system is administered by NCES and that we apply it because it applies stronger protections. I think that CIPSEA is a good thing to talk about when we talk about the security of the system.

Question: **How does CIPSEA and some of the other protections we've discussed relate to the Commission on Evidence-Based Policymaking recommendations?**

> Answer: I was on the commission's staff for the past year. The Commission on Evidence-Based Policymaking was tasked by Congress and POTUS to evaluate ways to improve

the availability and use of data for evidence based policymaking purposes. From the very beginning, the commissioners saw privacy and confidentiality as the center point of their work. They really focused extensively on privacy concerns at all stages of their deliberation. CIPSEA was at the center of those discussions. CIPSEA provides a distinction between statistical and non-statistical purposes which was essential to the commissioner's recommendations. It provides the penalties for misuse or unauthorized/willful disclosures, etc. The commission issued a number of recommendations in their report, and they sought to frame their recommendations within the framework on CIPSEA. The report puts forward a set of changes to the federal statistical system and the way the government collects evidence-based data.

Question: **As a follow up to Mamie's question, can you provide some examples at ED of collections that qualify as statistical collections under CIPSEA?**

Answer: I defer to my colleagues at NCES. As I understand it, the surveys and statistical collections that NCES collect and conduct have confidential protections equivalent to CIPSEA protections. I believe there is a difference in the educational sciences reform act of 2002. Additionally, I believe there are some limits for national security reasons and caveats for the 2015 Cybersecurity Act.

Question: **Please speak more about the secure multi-party computation...**

Answer: (HAWES) There are challenges with secure multi-party computation. You are performing the linkages and analysis without seeing the raw data. The quality of the record linkages may be dubious as far as being able to ascertain what the linkages actually are. This is a technology that may need some work before implementing. (SADLER) Added security enhancement may be secure multi-party computation which has the goal of creating methods for parties to jointly compute a function over their inputs while keeping those inputs private.