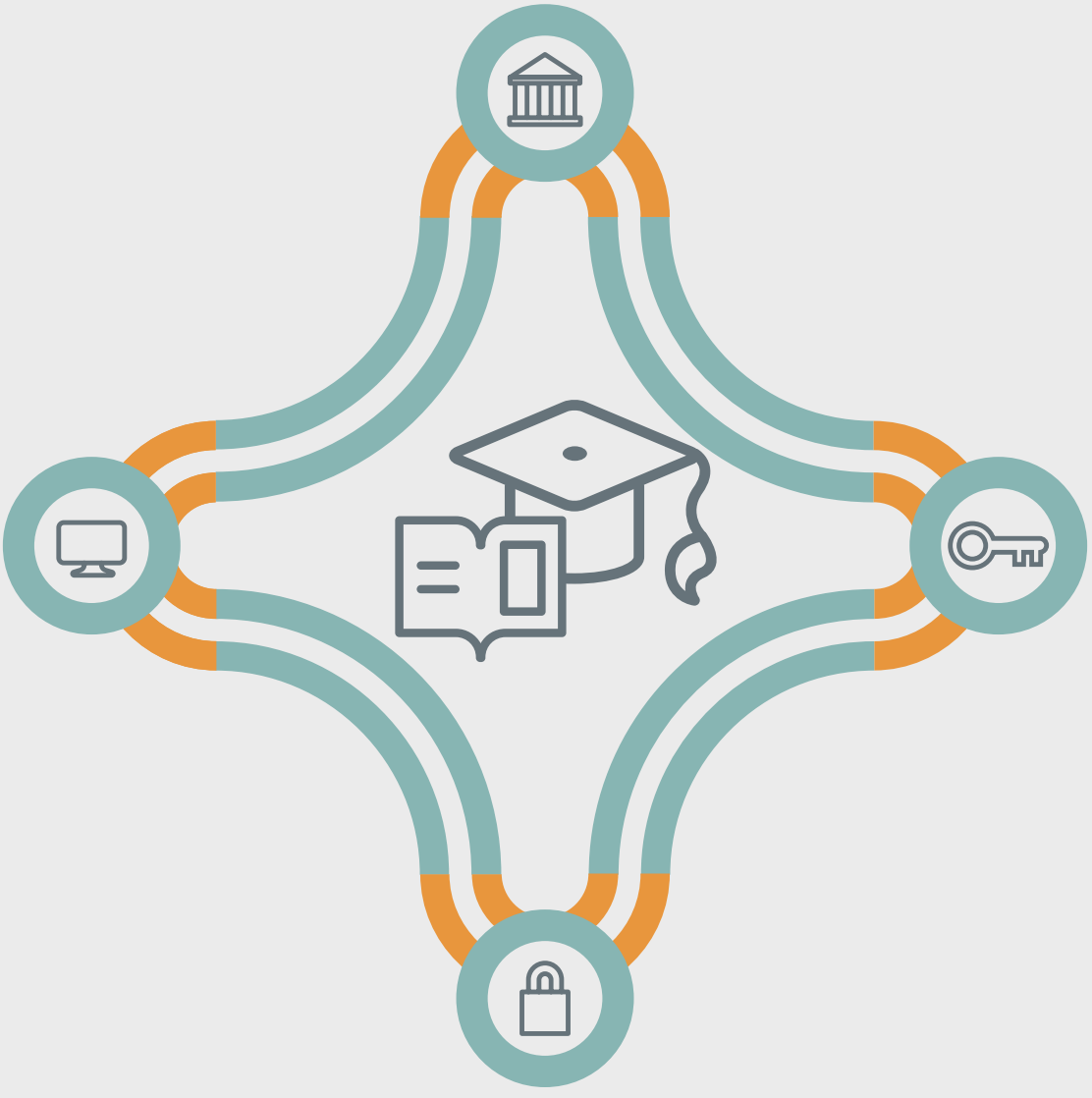
Protecting Privacy and Information Security in a Federal Postsecondary Student Data System

AUTHOR: JOANNA LYN GRAMA, VANTAGE TECHNOLOGY CONSULTING GROUP[1]

MAY 2019

VANTAGE Technology Consulting Group

POSTSEC DATA



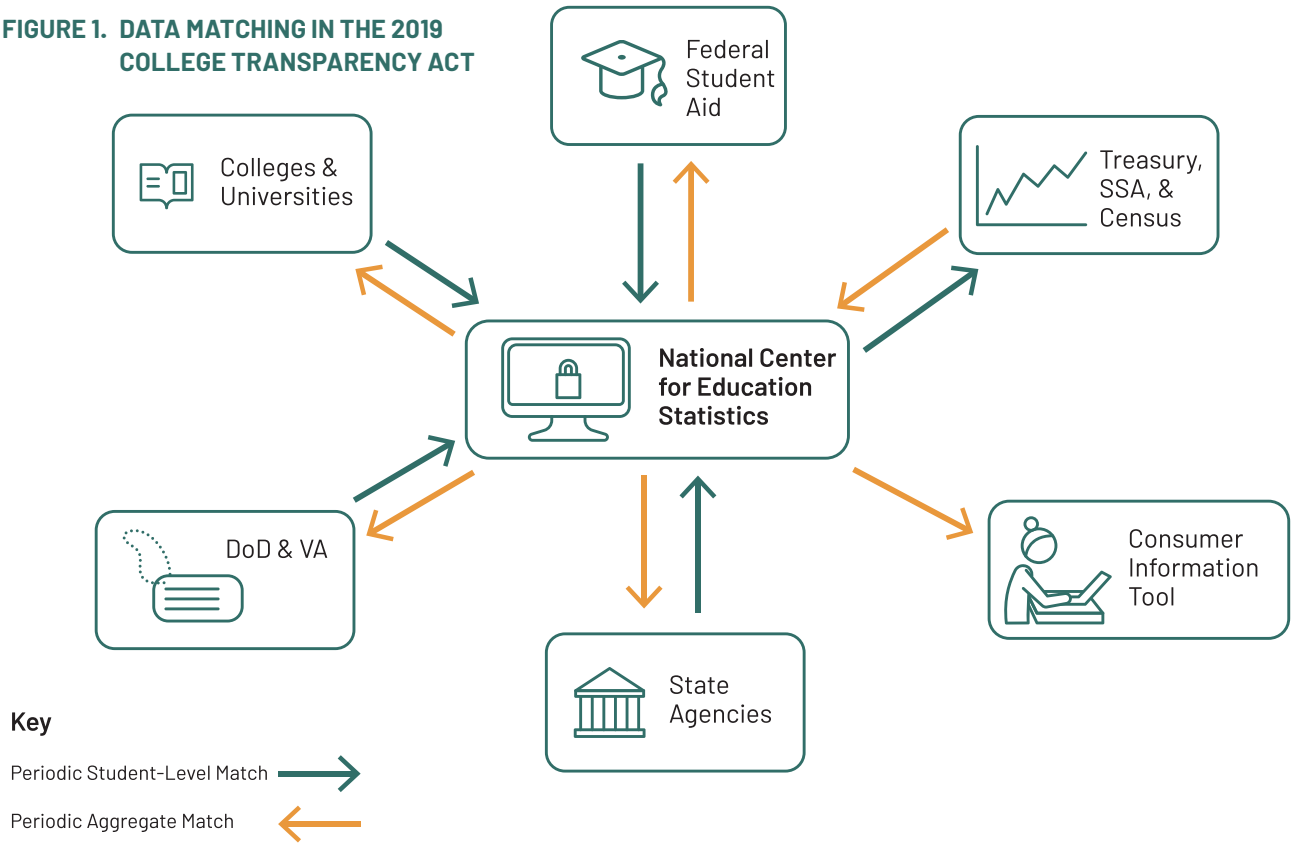
Joanna Lyn Grama, JD, CISSP consults on higher education information security and privacy issues at Vantage Technology Consulting Group.

This paper is part of the larger series *Protecting Students, Advancing Data: A Series on Data Privacy and Security in Higher Education*. In August 2018, the Institute for Higher Education Policy (IHEP) first convened a Privacy and Security Advisory Board of privacy and security experts and higher education experts to explore some of the most pressing data privacy and security issues of the day. The resulting paper series serves as a resource for policymakers as they develop sound postsecondary data policy and centers privacy and security as a top priority. This report is based on research with support from Arnold Ventures. The findings and conclusions contained within are solely those of the author.

Introduction

In March 2019, a bipartisan group of U.S. Senators introduced legislation to overturn a longstanding ban on the creation of a federal data system that would measure employment and graduation outcomes of college students. Creating a federal postsecondary student-level data system (referred to in this paper as a student-level data network or SLDN), as envisioned by the 2019 College Transparency Act (CTA)[2], could be a gamechanger for students, parents, institutions, and policy makers who currently do not have a full and complete picture of college access and outcomes measures. While data is already available—colleges and universities, multistate collaboratives, private organizations, and the federal government all collect, share, and use different types of postsecondary data—the infrastructure is fragmented, disconnected, and uncoordinated. As a result, the available dataset is inadequate to meet the needs of all who depend on it.[3]

FIGURE 1. DATA MATCHING IN THE 2019 COLLEGE TRANSPARENCY ACT



The 2019 CTA envisions a federal postsecondary SLDN, developed and maintained within the National Center for Education Statistics (NCES), as shown in *Figure 1*.[4] Located within the Department of Education, NCES is the primary federal entity for collecting and analyzing U.S. education data.[5] Recognizing the importance of security and privacy considerations in a system holding student data, the newly introduced 2019-version CTA[6] mandates that the federal SLDN created under the law ensures data privacy and security in a number of ways. For instance, the 2019 CTA specifically references the applicability of federal information security laws.[7]

This paper outlines the privacy and information security laws that pertain to federal information systems and discusses special issues that should be addressed in a federal SLDN.

When thinking about information security and privacy concepts within the federal SLDN, it is important to understand the following terms:

- **Federal information system:** As its name implies, a federal information system is an information system that is used or operated by a federal agency or on behalf of a federal agency. They include information technology (IT) resources used for the "collection, processing, maintenance, use, sharing, dissemination, or disposition of information."[8]
- **Information privacy:** The right of an individual to control his or her own data and to specify how those data are collected, used, and shared. For governmental agencies, protecting information privacy means that data is collected, used, and stored in accordance with an understood set of privacy principles.
- **Information security:** The study and practice of protecting data in all its forms (e.g., whether stored in an IT system or reduced to paper or another physical medium). It means making sure that information is available only to those who need to use it (confidentiality), is ready for use when it is needed (availability), and remains correct and accurate throughout its lifecycle (integrity).
- **Personally identifiable information (PII):** Information that identifies a specific individual, PII can include a single piece of information used alone, such as a person's name or Social Security Number (SSN). Or it can be data elements that, when combined together, can identify a particular individual. Common personally identifiable data elements include name, SSN, physical address, email address, zip code, race, age, gender, GPS location, telephone number, college or university identification number, and account numbers. Different laws may include different elements in their definitions of PII, so the applicable legal definition can vary.

Protecting Privacy in Federal Information Systems

Two main laws protect the privacy of data used by the federal government: The Privacy Act of 1974[9] and the E-Government Act of 2002.[10] The Privacy Act regulates the collection, use, and disclosure of records about individuals when those records are retrieved by a personal identifier. The E-Government Act requires the federal government to assess the privacy impact to PII maintained in federal information systems. In addition, the Confidential Information Protection and Statistical Efficiency Act of 2002 includes additional privacy protections regarding statistical data that apply to agencies like NCES.

THE PRIVACY ACT OF 1974

The Privacy Act of 1974, the foundational public-sector privacy law, was designed to protect the privacy of records created and used by the federal government. The Privacy Act states the rules that a federal agency must follow to collect, use, transfer, and disclose an individual's PII. It also requires agencies to collect and store only the minimum information that they need to conduct their business. Agencies that violate the Privacy Act can be subject to civil and criminal penalties.

The Privacy Act applies only to government records that contain the personal information of U.S. citizens and permanent residents,[11] are held in a system of records, and are retrievable by a personal identifier. Under the law, records are "any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph."[12] Records must identify a specific individual. A system of records is a group of records in a

federal agency's control "from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."[13] The most common personal identifiers are name and SSN. A system of records is a record management system, whether it is paper- or electronic-based.

Under the Privacy Act, government agencies have rules that they must follow when they maintain a system of records that includes PII. In many respects, the rules stated in the Privacy Act are a set of fair information practices regarding federal agency collection of PII. While court cases continue to test and define the scope of these rules, they can be generalized as follows:

- Federal agencies must collect only the PII they need to carry out a specific statutory purpose;
- At the time PII is collected, federal agencies must explain to an individual what information is being collected, why it is needed, and how it will be used;
- Federal agencies must ensure that the records collected are used only for the reasons originally specified when that data was collected; otherwise, the agency must seek the individual's permission when the use of that data for another purpose is needed;
- Federal agencies must allow individuals to see the records kept on that person and allow the individual an opportunity to correct inaccurate records; and
- Federal agencies must protect the security and confidentiality of the records that they collect.[14]

The notice requiring federal agencies to give the public formal written notice about any records that it keeps that can be, and are actually, retrieved using a personal identifier.[15] This notice is called a system of records notice (SORN). It describes the data being collected and how they will be used. A SORN also must describe how an individual can access or correct any incorrect PII held in the system of records. Federal agencies must publish their SORNs in the Federal Register and must also make them available online. For example, you can find SORNs for the U.S. Department of Education here: https://www2.ed.gov/notices/ed-pia.html

Under the Privacy Act, the federal government cannot disclose any of the PII that it collects about an individual unless the underlying individual gives consent or the disclosure is made pursuant to one of twelve broad statutory exemptions[16]:

- Made to a federal agency employee who needs the record to perform his or her job duties;
- Required under the Freedom of Information Act;
- Made for an agency's routine use (i.e., disclosure of a record for a purpose that is compatible with the purpose for which the record was collected);
- Made to the U.S. Census Bureau to perform a survey;
- Made for statistical research or reporting, and all personally identifiable data has been removed;
- Made to the National Archives and Records Administration because the record has historical value;
- Made in response to a written request from law enforcement or regulatory agencies for civil or criminal law purposes;
- Made to protect a person's health or safety;
- Made to Congress;
- Made to the U.S. Comptroller General in the course of the performance of the duties of the U.S. Government Accountability Office;
- Made in response to a court order; or
- Made to a consumer reporting agency for certain permitted purposes.

The 2019 CTA states a number of permissible disclosures of data from the SLDN, none of which include PII. Under the 2019 CTA, the Commissioner of NCES is specifically directed to "use appropriate statistical disclosure limitation techniques necessary to ensure that the data released to the public cannot include [PII] or be used to identify specific individuals."[17] In addition, no data collected for the SLDN may be sold to a third party[18], and the 2019 CTA places limitations on how other federal agencies may use the SLDN data.[19]

THE E-GOVERNMENT ACT OF 2002

The E-Government Act was among the first federal laws to comprehensively address information privacy and security issues in federal information technology systems. It complements the Privacy Act of 1974 and was intended to promote access to electronic government resources. The E-Government Act recognized that advancements in technology had created an environment where public and personal data was more readily accessible to all and that the federal government needed to use technology to enhance its services and processes in order to be more efficient and effective. The Act contains a variety of provisions related to how the federal government manages its IT resources. Chief among the E-Government Act's information privacy requirements is Section 208, which introduces the use of privacy impact assessments (PIAs).

Section 208 of the E-Government Act requires federal agencies to complete and publish a PIA before the agency develops, buys, or sub-contracts an IT system that collects PII.[20] Agencies also must perform PIAs any time their IT systems are changed, modified, or updated in ways that introduce new privacy risks. The purpose of completing a PIA is to help a federal agency identify and mitigate privacy risks when an IT system that contains PII is being first developed and to continue to mitigate such risks throughout the entire development lifecycle of that system.

The U.S. Office of Management and Budget (OMB), which is responsible for issuing guidance to federal agencies on implementing the E-Government Act's privacy provisions, has specified that PIAs must analyze and contain the following information:

1. What information is to be collected;
2. Why the information is being collected;
3. Intended use of the information;
4. With whom the information will be shared;
5. What opportunities individuals have to decline to provide information or to consent to particular uses of the information and how individuals can grant consent;
6. How the information will be secured; and
7. Whether a system of records is being created under the Privacy Act.[21]

Since it is intended as a decision-making tool, the PIA must contain a level of analysis and detail sufficient for the nature of the information to be collected and the complexity of the underlying IT system to be readily apparent. It must also fully analyze the privacy risks to the data and IT system. Finally, the PIA must document the privacy-related choices that an agency made regarding its IT systems as a result of performing the PIA.[22] Federal agencies must publish their completed PIAs in the Federal Register and make them available online. For example, PIAs for the U.S. Department of Education are available here: https://www2.ed.gov/notices/pia/index.html

The Privacy Act and the E-Government Act have some notable differences. For instance, the E-Government Act is tailored to federal IT operations, where the Privacy Act is not. In addition, the Privacy Act is focused on protecting the privacy rights of individuals who are U.S. citizens or lawful permanent residents, while the E-Government Act allows federal agencies to expand the definition of individual to include non-U.S. citizens. Finally, while they appear to have similar goals and contain similar information, the system of records notices required under the Privacy Act and the PIAs required under the E-Government Act are not the same. *Table 1* compares SORN and PIA elements as specified under their respective acts. Note that the SLDN envisioned by the 2019 CTA would require NCES to prepare and complete both a SORN and a PIA.

TABLE 1: COMPARISON OF SORN AND PIA ELEMENTS

	SYSTEM OF RECORDS NOTICE (SORN)	PRIVACY IMPACT ASSESSMENT (PIA)
LEGAL AUTHORITY	The Privacy Act of 1974	The E-Government Act of 2002
WHAT IT IS	A legal notice that describes government records subject to the Privacy Act, it provides notice to U.S. citizens and lawful permanent residents on how to access, correct, and amend their records.	A decision-making tool used to identify and mitigate privacy risks, it helps the public understand when an agency collects PII, why it is being collected, and how it will be used, shared, accessed, secured, and stored.
WHEN REQUIRED	A SORN is required when: • Records are maintained by a federal agency, • The records contain PII about a U.S. Citizen or lawful permanent resident, and • The records are retrieved by a personal identifier.	A PIA is required before: • A program or system containing PII is developed or purchased or • An agency initiates a new collection of PII that will be collected, maintained, or disseminated using IT.
CONTENTS	• System name • System security classification • System location • PII included in the system • Legal authority for system creation • How the PII in the system is collected • How the PII in the system will be used • How the PII in the system can be retrieved (i.e., the unique identifier) • How PII in the system will be secured • How individuals can access, correct, and amend their records.	• What PII is to be collected • Why the PII is being collected • The intended use of the PII • How the PII will be shared • What notice or opportunities individuals have to decline to provide PII • How PII in the system will be secured • Whether a system of records is being created under the Privacy Act.
WHERE PUBLISHED	Federal Register and agency websites	Federal Register and agency websites

FEDERAL DATA PROTECTION LAWS FOR INSTITUTIONS AND NON-GOVERNMENTAL AGENCIES

While the CTA envisions a federal SLDN, developed and maintained within NCES, some parts of the postsecondary education data infrastructure lie outside of the federal government; notably colleges and universities, multistate collaboratives, and private organizations. A myriad of state and federal laws will apply to how data is collected and shared within the federal SLDN. The following federal laws may apply to how higher education institutions and non-governmental agencies collect and use data that may be used within the federal SLDN:

- **The Family Educational Rights and Privacy Act of 1974 (FERPA)**[23] is designed to protect students and their families by ensuring the privacy of student educational records. Educational records are agency or institution-maintained records containing personally identifiable student and educational data. FERPA applies to primary and secondary schools, colleges and universities, vocational colleges, and state and local educational agencies that receive funding under any program administered by the U.S. Department of Education. FERPA contains provisions specifying how access, amendment, and disclosure of education records must be handled. Currently, FERPA does not contain specific information security standards that institutions and agencies must use to protect student educational records.
- **The Health Insurance Portability and Accountability Act of 1996 (HIPAA)**[24] requires covered entities (typically medical and health insurance providers and their associates) to protect the security and privacy of health records. This law is often implicated in conversations about student data when institutions have a campus medical center and student medical records are integrated with student educational records (which are protected under FERPA).
- **The Gramm-Leach-Bliley Act (GLBA)**[25] applies to financial institutions and contains privacy and information security provisions that are designed to protect consumer financial data. This law also applies to how institutions collect, store, and use student financial records (e.g., records regarding tuition payments and/or financial aid) containing PII.
- **The Fair and Accurate Credit Transaction Act of 2003 (FACTA or "Red Flags Rule")**[26] requires entities engaged in certain kinds of consumer financial transactions (largely credit transactions) to be aware of the warning signs of identity theft and to take steps to respond to suspected incidents of identity theft. Like GLBA, this law applies to how institutions collect, store, and use student financial records.

THE CONFIDENTIAL INFORMATION PROTECTION AND STATISTICAL EFFICIENCY ACT OF 2002

The Confidential Information Protection and Statistical Efficiency Act (CIPSEA)[27] was enacted to establish confidentiality protections for information collected for statistical purposes by U.S. statistical agencies like NCES. The 2019 CTA invokes CIPSEA, which was enacted as part of the E-Government Act of 2002. CIPSEA is a relatively short act and states that all PII supplied by individuals (either directly or from another organization) to a federal agency for statistical purposes must be kept confidential and only be used for statistical purposes, unless the underlying individual specifically consents to the disclosure.[28] Violating CIPSEA has severe penalties. Any agency employee that willfully discloses any PII in a manner not permitted by CIPSEA can be imprisoned for up to five years and fined up to $250,000.[29]

CIPSEA also acknowledges that many federal statistical agencies issue confidentiality pledges that explicitly state that the PII provided to the agency will only be used for statistical purposes and seen by statistical agency personnel or their agents. The purpose of these pledges is to enhance the trust between the statistical agency and entities providing PII to the agency. NCES pledges of confidentiality are maintained within its statistical standards documentation.[30]

Protecting Information Security in Federal Information Systems

The Federal Information Security Management Act of 2002 (FISMA)[31] is the main law specifying how federal agencies must protect the security of federal information technology systems and the data contained within those systems. In addition to FISMA requirements, federal agencies must follow standards issued by the National Institute of Standards and Technology (NIST) in implementing their FISMA-required information security programs. Finally, should an agency experience a breach of PII, they must follow OMB guidance on whether to provide notification to affected individuals.[32]

THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002

Specifically focused on information technology systems, FISMA was enacted as part of the E-Government Act of 2002.[33] FISMA was most recently updated and modernized in 2014 by the Federal Information Security Modernization Act of 2014 (also called FISMA; for the purposes of this paper, FISMA will only be used to refer to the Federal Information Security Management Act of 2002). FISMA imposes mandatory rules that a federal agency must follow for all IT systems used or operated by that agency.[34] It also provides federal agencies with a framework for how they should implement and manage agency information security programs. FISMA compliance is mandatory for all federal agencies, so it would apply to the National Center for Education Statistics' creation and management of an SLDN. It also applies to contractors of federal agencies and any other organization supporting a federal agency IT system.[35] Federal agency compliance with FISMA is not a "one and done" project; instead, it can best be thought of as a continuous improvement process designed to secure federal IT systems.

FISMA requires federal agencies, including statistical agencies like NCES, to implement risk-based information security programs for their IT systems. Under the law, agencies must:

- Designate a senior official to be in charge of its information security efforts;
- Conduct periodic risk assessments of the harm that could result from a breach of information security;
- Create policies and procedures;
- Implement subordinate plans to protect the agency's infrastructure;
- Conduct security awareness training;
- Regularly test and evaluate the effectiveness of the agency information security program;
- Implement a process for remediating information security deficiencies;
- Create an incident response process;
- Ensure that plans are in place to ensure continuity of operations for agency information systems; and
- Submit a yearly report to the OMB, Department of Homeland Security (DHS) and several congressional agencies regarding the adequacy and effectiveness of its information security program.[36]

In addition to the program requirements stated above, agencies must also have a yearly independent evaluation of its information security program (the results of which are included in its yearly report). For most agencies, this audit is performed by its inspector general.[37] The report also must include information on any information security incidents or breaches of PII that happened within the past year.[38]

FISMA oversight responsibilities are delegated to the Director of the OMB and to the Secretary of the DHS.[39] Among other duties, the Director and the Secretary are responsible, in coordination with the National Institute of Standards and Technology (NIST), for creating and requiring agency compliance with information security standards and guidance.

THE ROLE OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Agencies must follow NIST standards and guidelines in implementing their information security programs.[40] An agency within the Department of Commerce, NIST develops the standards and guidelines that federal agencies, and their contractors, must follow to meet their FISMA obligations to protect the information security of agency information systems and assets.[41] NIST creates two main types of documents:

1. Federal Information Processing Standards (FIPS), which establish mandatory requirements for information processing, and
2. NIST Special Publications (SPs), which provide technical guidance for developing information security programs

NIST creates FIPS when a compelling reason exists — either a statutory requirement or an identified federal requirement for cybersecurity that cannot be found in other industry best practices. Since they are formal rules, NIST must follow the process outlined in the Administrative Procedures Act for creating a FIPS. FIPS are reviewed every five years for continued applicability.[42] Currently, there are nine FIPS documents.[43]

NIST Special Publications provide cybersecurity guidance and recommendations. The NIST SP 800 series of documents addresses how cybersecurity and privacy should be implemented in federal information systems in particular. The NIST SP 800 series has over 100 documents, many of which federal agencies are required to follow.

The main NIST publications that federal agencies must consult and follow for meeting their FISMA information security obligations are:

- **FIPS 199 – Standards for Security Categorization of Federal Information and Information System.**[44] This standard helps federal agencies categorize their data and IT systems. It specifies a low, medium, and high rating schema. Federal agencies then use these classifications to assess the risk to their information systems.
- **FIPS 200 – Minimum Security Requirements for Federal Information and Information Systems.**[45] This standard states the minimum security requirements for information and information systems that federal agencies must follow. These minimum requirements cover seventeen different information security topic areas. This standard also requires federal agencies to use a risk-based process for selecting information security controls for their environments.
- **NIST 800-37 – Guide for Applying the Risk Management Framework to Federal Information Systems.**[46] This guide, revised most recently in 2018, walks federal agencies through a seven-step risk management process to ensure FISMA compliance for their information systems.
- **NIST 800-53 – Security and Privacy Controls for Information Systems and Organizations** *(see Sidebar)*[47] This publication is a catalog of potential information security and privacy controls to implement in federal information systems. Federal agencies are required to implement specialized controls based on the underlying classifications of their information systems (as determined via FIPS 199). A new version of this publication, revision 5, is expected in 2019.

This suite of mandatory and suggested information security requirements results in a complicated information security framework that federal agencies, like NCES, must follow with respect to their IT systems.

OMB BREACH NOTIFICATION REQUIREMENTS

Federal agencies have a number of different rules that they must follow for reporting information security and privacy incidents to the OMB and different federal agencies. The rules are intended to ensure that the government proactively manages potential incidents to minimize disruptions to federal information systems and to protect national security. Federal agencies also are required to prepare their response plans for a breach of personally identifiable information.[48]

OMB memorandum 17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information," sets forth the process for how federal agencies must prepare for and respond to a breach of PII. The OMB guidance takes a deliberately expansive view of PII, stating that PII is "information that can be used to distinguish or trace an

NIST SPECIAL PUBLICATION 800-53

NIST Special Publication 800-53 states the minimum security and privacy controls that federal agencies should follow to secure federal information systems. First published in 2005 and revised four — soon to be five — times, NIST Special Publication 800-53 is a catalog of security and privacy controls that can be implemented within federal agencies' information systems to protect those systems from a number of different risks such as hostile attacks or human error. NIST 800-53 Revision 4 has eighteen families of security controls, and within each family is guidance on how to select appropriate safeguards to meet an agency's information security goals. There are over 500 separate information security controls in NIST 800-53. The control families are:

- Access Control,
- Audit and Accountability,
- Awareness and Training,
- Configuration Management,
- Contingency Planning,
- Identification and Authentication,
- Incident Response,
- Maintenance,
- Media Protection,
- Personnel Security,
- Physical and Environmental Protection,
- Planning,
- Program Management,
- Risk Assessment,
- Security Assessment and Authorization,
- System and Services Acquisition,
- System and Communications Protection, and
- System and Information Integrity.

The controls listed in NIST 800-53 range from administrative (e.g., policy-based) controls to highly technical controls. For example, awareness and training control AT-2 is an administrative control and states: "The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors): (a.) As part of initial training for new users; (b.) When required by information system changes; and (c.) [Organization-defined frequency] thereafter." Conversely, configuration management control CM-7 is more technically focused and reads, "The organization: (a.) Configures the information system to provide only essential capabilities; and (b.) Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [Organization-defined prohibited or restricted functions, ports, protocols, and/or services]."

individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."[49] The definition of breach is a common-sense one, referring to any "loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for any other than authorized purpose."[50] The OMB memo is quick to point out that a breach can occur both through unauthorized intrusion into information technology systems and also through the loss of physical documents containing PII.

Agencies have some discretion on whether and how to provide notification and services to individuals who are affected by a breach of their PII. Among a number of factors, agencies must weigh the risk of harm to the individual, the number of individuals impacted by a breach event (and whether any of those individuals are part of a vulnerable population), any guidance or services the agency might want to provide as a result of the breach, and over-notification concerns. The agency must also weigh whether another law requires notification (e.g., the Health Insurance Portability and Accountability Act). If an agency chooses to make a notification, the OMB requires that it make that notification in a timely manner, include enough detail about the breach so that individuals can protect themselves and their information, and make the notification in a way that reflects the urgency of the underlying situation.[51]

Special Considerations for an SLDN Federal Information System

The federal SLDN authorized by the 2019 College Transparency Act would be a federal information system that will be subject to federal information security and privacy laws. The application of the laws discussed in this paper would begin to lay the foundation for a trustworthy and secure federal SLDN that protects student PII while still allowing good data to help us understand student postsecondary access and outcomes measures. For example, a PIA, assessing the privacy risks to this type of system, would need to be completed before the system is developed or purchased. A system of records notice would need to be published if the records in the SLDN could be retrieved by a personal identifier (which is presumably possible). And finally, information security and privacy controls specified by NIST would need to be implemented within the SLDN to keep the data in that information system protected and secure.

While a solid foundation for a security- and privacy-minded federal SLDN is outlined in the 2019 CTA *(see Sidebar)*,[52] authorization of a federal SLDN is not a complete panacea to information security and privacy concerns surrounding the collection and use of student data. Federal agency information systems and the government technology infrastructure are notoriously complex. It cannot be assumed that just because an information system is a federal information system that it is secure. Instead, what is noteworthy is that extensive IT, information security, and information laws, regulations, rules, and guidance are available to help protect federal information systems. This framework will guide the federal practices that secure student PII.

Addressing security and privacy in the federal SLDN is only one part of the information security and privacy inquiry, however. The current national postsecondary education infrastructure is complex and has many stakeholders, participating entities, and underlying information technology systems. Data will flow between these entities, sometimes in identifiable formats, such

The 2019 CTA includes a number of different provisions designed to ensure the security and privacy of data contained in a federal SLDN. Among its provisions, the act:

- Directs NCES to develop and maintain a security- and privacy-protected SLDN consistent with federal information security laws. 2019 CTA § (I)(1)(C)(iv).
- Requires NCES to create and regularly revise its privacy, security, and access guidelines that govern the use and disclosure of data collected for the SLDN. 2019 CTA § (I)(8).
- Directs NCES to follow federal data minimization standards to ensure that any PII collected is necessary to meet the purpose and goals of the SLDN. 2019 CTA § (I)(1)(C)(v).
- Creates a Postsecondary Student Data System Advisory Committee, that includes the Department of Education's chief privacy officer and chief security officer, as well as other individuals with data privacy and security expertise, to advise on data elements to be included in the SLDN. 2019 CTA § (I)(2)(B).
- Specifies the type of PII that may never be included in the federal SLDN, to include elements such as health data, citizenship status, and political status. 2019 CTA § (I)(2)(B). 2019 CTA § (I)(2)(F).
- Outlines permissible uses of SLDN data and states the consequences of unlawful willful disclosure. 2019 CTA § (I)(5)(E); § (I)(7).
- Prohibits the use of the SLDN for law enforcement activities or any other activity that might result in adverse action against a student. 2019 CTA § (I)(5)(E).
- Directs NCES to provide notice to students outlining which data are collected and used in the SLDN. 2019 CTA § (I)(1)(C)(vi).
- Requires NCES to provide students with a process to access their information and correct inaccuracies. 2019 CTA § (I)(3)(C)(iv).

as from an institution to the federal SLDN to provide enrollment, price, and completion data at the student level. Other times that data will flow in aggregate formats, such as from the SLDN to a state agency to provide college transfer, completion, and workforce outcomes. In order to provide meaningful information to students, parents, and policy makers, data from these different systems must be contributed to the federal SLDN in a way that allows for matching, by some common key or identifier, throughout the entire infrastructure. Rules will need to be established to ensure that only the minimum data needed to answer important questions about college access, cost, and success are collected and analyzed. The entire ecosystem that will support the federal SLDN will need to be tended carefully to ensure its success.[53] Given that multiple entities, some private and some governmental, will contribute, use, and analyze data within the infrastructure, data governance structures and clear information security and privacy practices will need to be agreed to and followed by all participating entities.[54]

If enacted, the 2019 CTA provides for a four-year transition period to develop and implement the federal SLDN. During this transition period, NCES should:

- Immediately constitute and actively engage with the CTA-created Postsecondary Student Data System Advisory Committee during the entire systems development process to ensure that security and privacy provisions are embedded in the SLDN from design to implementation.
- Outline the systems development lifecycle approach that it will follow in creating the SLDN, ensuring conformity with any Department of Education lifecycle management specifications.[55]
- Consult best practices guidance regarding security and privacy practices during the systems development lifecycle.[56]
- Follow the privacy and security requirements set out in the 2019 CTA.
- Adhere to federal privacy and information security laws regarding the creation and operation of federal IT systems.

CONCLUSION

The amount of student and family PII collected by and linked within a federal SLDN could give unprecedented insight into questions of college access, affordability, and student outcomes. Despite the benefits of ensuring access to accurate, timely, and high-quality aggregate data about student outcomes, ensuring the adequate security of such a system and protecting the privacy of individuals who have identifiable data in that system are of utmost importance. The 2019 CTA acknowledges these concerns and provides a solid foundation for a security- and privacy-minded federal postsecondary SLDN with the direction that the NCES develop and maintain such a system consistent with federal information security and privacy laws.

Endnotes

1 Joanna Lyn Grama, JD, CISSP consults on higher education information security and privacy issues at Vantage Technology Consulting Group. She is a frequent speaker on a variety of information security, privacy, risk, and compliance topics. This paper does not constitute legal advice. Entities seeking advice on the application of any of the laws mentioned in this paper should consult with legal counsel.

2 College Transparency Act of 2019, S.800, 116th Congress (2019-2020). Retrieved from: https://www.congress.gov/bill/116th-congress/senate-bill/800/text.

3 Roberson, A.J., Rorison, J., and Voight, M. (2017). A Blueprint for Better Information: Recommendations for a Federal Postsecondary Student-Level Data Network. Retrieved from Institute for Higher Education Policy website: http://www.ihep.org/sites/default/files/uploads/docs/pubs/a_blueprint_for_better_information_ihep.pdf.

4 2019 CTA § (I)(1)(A).

5 20 U.S. Code § 9541. All U.S. code citations herein retrieved from https://www.govinfo.gov/app/collection/USCODE.

6 Note that the version of the College Transparency Act (CTA) introduced in 2019 contains a number of privacy and security references that were not part of the 2017 version of the CTA. The provisions added to the 2019 version make clear the government's intention that adequate security and privacy protections be incorporated into the new system as it is developed.

7 2019 CTA § (I)(1)(C)(iv). The 2019 version of the College Transparency Act (CTA) includes numerous revisions intended to showcase the importance of security and privacy in an SLDN. These are welcome additions to the CTA.

8 44 U.S. Code § 3502.

9 Privacy Act of 1974, 5 U.S. Code § 552a.

10 Pub. L. No. 107-347, 116 Stat. 2899, codified in scattered sections throughout U.S. Code vol. 44.

11 5 U.S. Code § 552a(a)(2).

12 5 U.S. Code § 552a(a)(4).

13 5 U.S. Code § 552a(a)(5).

14 5 U.S. Code § 552a(e).

15 5 U.S. Code § 552a(e)(4).

16 5 U.S. Code § 552a(b).

17 2019 CTA § (I)(5)(B).

18 2019 CTA § (I)(5)(C).

19 2019 CTA § (I)(5)(D).

20 Note that the E-Government Act defines individuals as U.S. citizens and lawful permanent residents, but that federal agencies may choose to extend the protections of the E-Government act to persons who are not citizens or lawful permanent residents of the United States. For example, the Department of Education has made this extension. See Department of Education Departmental Directive, OM: 6-108, Privacy: Section 208 of the E-Government Act of 2002 Policy and Compliance (September 6, 2016). Retrieved from https://www2.ed.gov/policy/gen/leg/foia/om-6-108.pdf.

21 Id., M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, Attachment B.

22 See Office of Management and Budget, M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, Attachment B (September 26, 2003). Retrieved from https://obamawhitehouse.archives.gov/omb/memoranda_m03-22.

23 Family Educational Rights and Privacy Act of 1974 (FERPA), U. S. Code, vol. 20, sec. 1232g (2012).

24 Health Insurance Portability and Accountability Act of 1996 (HIPAA), U.S. Code, vol. 42, sec. 1320d (2012).

25 Gramm-Leach-Bliley Act (1999) (GLBA), Title V of the Financial Services Modernization Act of 1999, U.S. Code, vol. 15, sec. 6801, et seq.

26 Fair and Accurate Credit Transaction Act of 2003 (FACTA), Pub L. 108-159, 117 Stat. 1952.

27 Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA), Title V of the E-Government Act of 2002. Note that in 2018, Congress enacted the Foundations of Evidence-Based Policymaking Act (Pub. L. 115-143). This act codifies CIPSEA in a new subchapter located at U.S. Code, vol . 44 sec. 3561 et seq.

28 44 U.S. Code § 3572 (2019).

29 44 U.S. Code § 3572(f) (2019).

30 See Section 4, Processing and Editing of Data, at https://nces.ed.gov/statprog/2012/

31 Federal Information Security Management Act of 2002 (FISMA), Title III of the E-Government Act of 2002, U.S. Code, vol. 44, sec. 3541 et seq.

32 Office of Management and Budget, M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017). Retrieved from: https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf

33 FISMA is Title III of the E-Government Act of 2002.

34 FISMA has a number of different requirements related to information security across the federal government. This paper only focuses on those requirements pertaining to the actions that federal agencies must take in managing their IT systems and creating their information security programs.

35 44 U.S. Code § 3553(a).

36 44 U.S. Code § 3554(b).

37 44 U.S. Code § 3555.

38 44 U.S. Code § 3554(c).

39 44 U.S. Code § 3553.

40 Note that non-federal agencies may, at their discretion, use NIST guidelines as best practices to improve their own information security programs.

41 15 U.S. Code § 278g-3.

42 See NIST, Procedures for Developing FIPS (Federal Information Processing Standards) Publications. Retrieved from https://www.nist.gov/itl/procedures-developing-fips-federal-information-processing-standards-publications.

43 See NIST, Current Federal Information Processing Standards (FIPS). Retrieved from: https://www.nist.gov/itl/current-fips

44 National Institute of Standards and Technology. (2004). Standards for Security Categorization of Federal Information and Information Systems, FIPS 199. Washington, DC: National Institute of Standards and Technology. Retrieved from: https://csrc.nist.gov/publications/detail/fips/199/final

45 National Institute of Standards and Technology. (2006). Minimum Security Requirements for Federal Information and Information Systems, FIPS 200. Washington, DC: National Institute of Standards and Technology. Retrieved from: https://csrc.nist.gov/publications/detail/fips/200/final

46 Joint Task Force Transformation Initiative. (2018). Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Special Publication 800-37r2. Washington, DC: National Institute of Standards and Technology. Retrieved from: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

47 Joint Task Force Transformation Initiative. (2015). Security and Privacy Controls for Federal Information Systems and Organizations, Special Publication 800-53r4. Washington, DC: National Institute of Standards and Technology. Retrieved from: https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

48 OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information. (Full citation at FN 22).

49 Id., OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information.

50 Id., OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information.

51 Id., OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information.

52 In addition to specifying that the SLDN must comply with FISMA requirements, the 2019 CTA also NCES to "use modern, relevant, privacy- and security-enhancing technology, and enhance and update the data system as necessary to carry out [its purpose]." 2019 CTA § (I)(1)(C)(iii).

53 For a review of ecosystem issues see Cubarrubia, A. and Perry, P. (2016). Creating a Thriving Postsecondary Education Data Ecosystem. Retrieved from Institute for Higher Education Policy website: http://www.ihep.org/sites/default/files/uploads/postsecdata/docs/resources/postsecondary_education_data_ecosystem.pdf

54 Grama, J. (2016). Understanding Information Security and Privacy in Postsecondary Education Data Systems. Retrieved from Institute for Higher Education Policy website: http://www.ihep.org/sites/default/files/uploads/postsecdata/docs/resources/information_security_and_privacy.pdf.

55 See Department of Education, Department Directive OC-1016 (2016). Lifecycle Management (LCM) Framework. Retrieved from Department of Education website, https://www2.ed.gov/digitalstrategy/Lifecycle_Management_(LCM)_Framework.pdf

56 Kissel, R., Stine, K., Scholl, M., Rossman, H., Fahlsing, J., Gulick, J. (2008). Security Considerations in the System Development Life Cycle, Special Publication 800-64r2. Washington, DC: National Institute of Standards and Technology. Retrieved from: https://csrc.nist.gov/publications/detail/sp/800-64/rev-2/final

Protecting Students, Advancing Data: A Series on Data Privacy and Security in Higher Education **is a project of the Institute for Higher Education Policy. This report was produced with support from Arnold Ventures. The views expressed in this report are solely those of the authors.**