Cyber Security Requirements for Institutions of Higher Education

Dr. Linda R. Wilbanks
Chief Information Security Officer
Federal Student Aid

Agenda

- Purpose
- Definitions of Key Terms
- Information Security 911
- Risk Management Framework
- What is at Risk?
- Data Protection Obligations
  - Dear Colleague Letter
  - Student Aid Internet Gateway (SAIG) Enrollment Agreement
  - HEA/FERPA/Contractual
  - FISMA Cyber Security Controls (NIST SP 800-53 Rev4)
  - Protecting CUI in NonFederal Systems (NSIT SP 800-171)
  - Gramm Leach Bliley Act (GLBA)
- Summary
- Questions

Purpose

To provide risk management guidance on IT security to institutions of higher education and their third-party servicers as they are obligated to:

- Protect data used in all aspects of the administration of the Title IV Federal student financial aid programs;
- Report all breaches resulting in loss of PII to FSA.

Definitions of Key Terms

- **Security incident** – Any event that compromised the confidentiality, integrity, or availability of an information asset. A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

- **"Data" breach** – An incident that resulted in confirmed disclosure, not just exposure, to an unauthorized party.

- **Personally Identifiable Information (PII)-** Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

- **Sensitive PII** is Personally Identifiable Information, which if lost, compromised, or disclosed without authorization could result in **substantial** harm, embarrassment, inconvenience, or unfairness to an individual.

911 for Information Security

- April 2015: Office of Personnel Management (OPM) was hacked resulting in two major breaches and PII (> 4 million) was stolen. Later investigation in June-August 2015 revealed a second breach occurred May– August 2014 resulting in a breach of **21.5 million** individuals (federal employees, contractors, others)

- Intruders gained access because two factor authentication was not in use

Resulting Actions

- Heightened awareness of cyber security enforcement
- New federally mandated policies, procedures, requirements
- Applicable to any organization that uses or transmits federal data
- Short enforcement times, must be implemented NOW

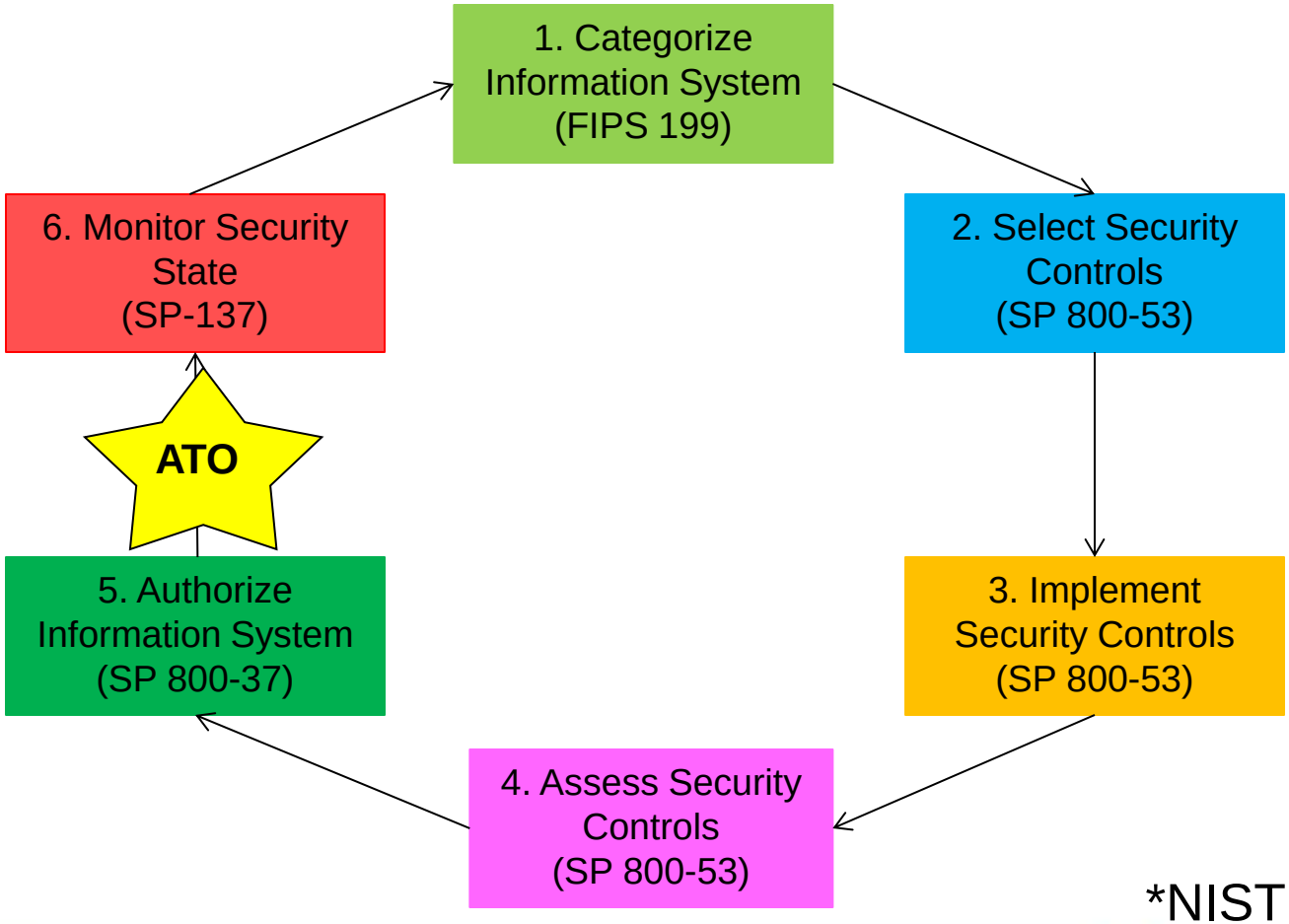
NO EXCEPTIONS FOR SECURITY ENFORCEMENT

What is at Risk?

Student and Parent Data at Risk

- Social media (Facebook, Twitter, LinkedIn)
- Mobile Devices (laptop, cellphones, tablets)
  - Lost/Stolen devices
  - Encryption
- Weak passwords and passwords written down and stored in an unsecure location
- Lack of monitoring credit card activity
- Improper disposal of mail with PII
- Public Wi-Fi provides easy compromise of credentials and data

Risk Management Framework*



*NIST SP 800-37

Data Protection Obligations

- Dear Colleague Letter
- HEA (Higher Education Act)
- FERPA (Family Educational Rights and Privacy Act)
- Student Aid Internet Gateway (SAIG) Enrollment Agreement
- Contractual Agreements
- FISMA Controls (NIST SP 800-53 rev 4)
- Protecting CUI (NIST SP 800-171)
- Gramm-Leach-Bliley Act (GLBA)

Dear Colleague Letter

- Publication Date: July 29, 2015
- Subject: Protecting Student Information
- Data breaches proliferating
- Cooperation of FSA Partners to implement strong security policies, controls, and monitoring is critical to protecting personally identifiable information and ensuring the confidentiality, availability, and integrity of Title IV financial aid information

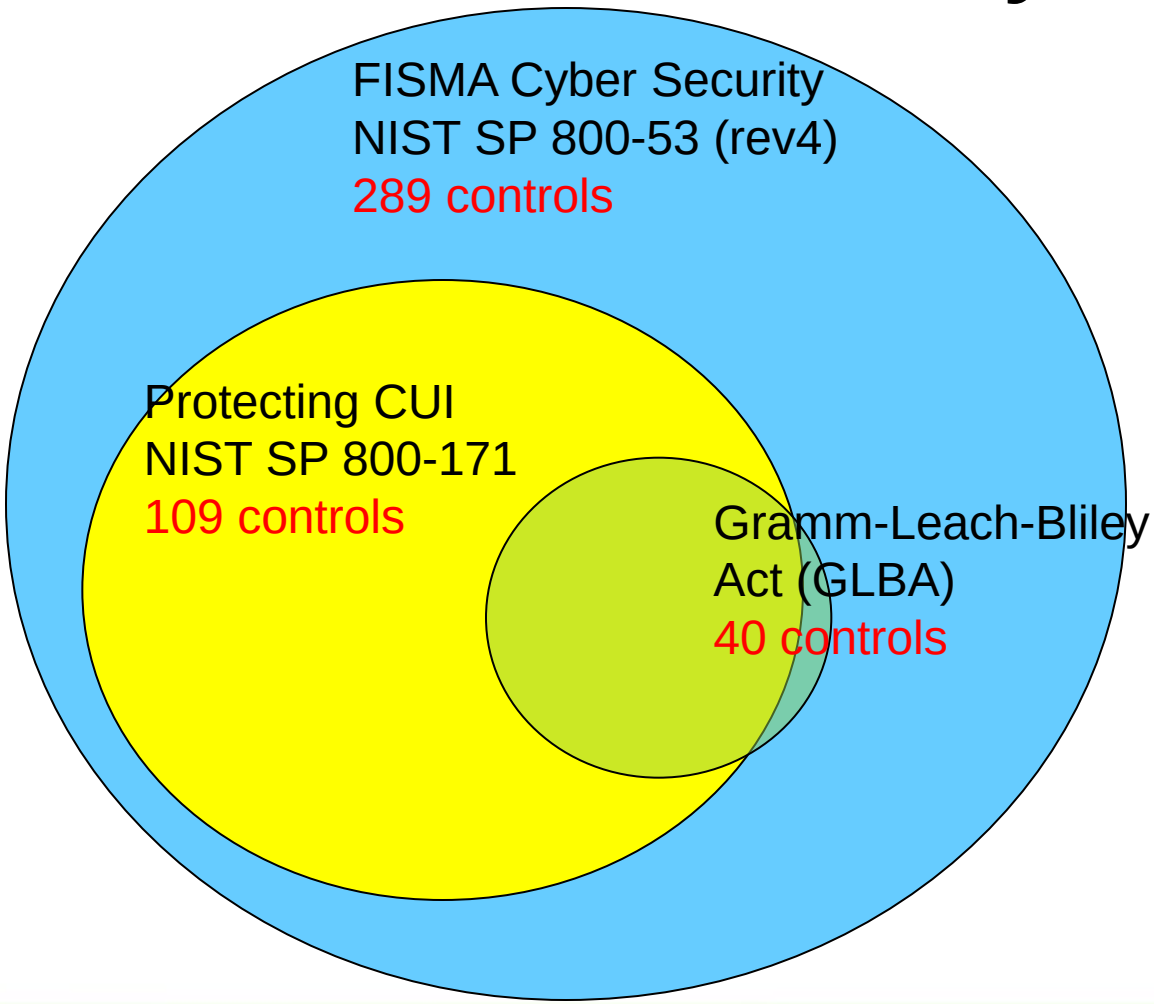
Student Aid Internet Gateway (SAIG) Enrollment Agreement

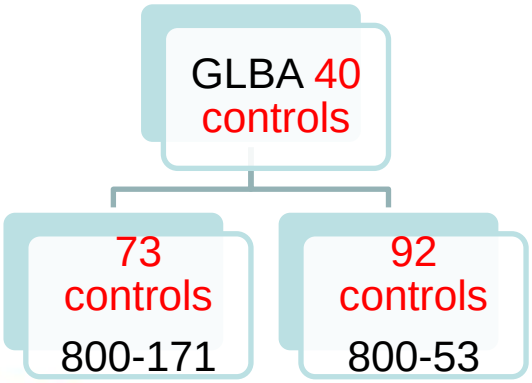
- Entered into by each Title IV participating institution
- Provides that each institution *"[m]ust ensure that all Federal Student Aid applicant information is protected from access by or disclosure to unauthorized personnel"*
- Identifies applicable regulations including
  - HEA (Higher Education Act)
  - FERPA (Family Educational Rights and Privacy Act)
  - Privacy Act of 1974 (Federal Agencies)
  - State data breach and privacy laws and potentially other laws

HEA/FERPA/Contractual

- HEA (Higher Education Act)
  - Sound administration of the Title IV programs would include satisfactory policies, safeguards, monitoring, and management practices related to information security
- FERPA (Family Educational Rights and Privacy Act)
  - Generally prohibits institutions from having policies or practices that permit the disclosure of education records or personally identifiable information (PII) contained therein without the written consent of the student. Any data breach resulting from a failure of an institution to maintain appropriate and reasonable information security policies and safeguards could also constitute a FERPA violation
- Contractual Agreements per 34 CFR § 668.25
  - The institution remains liable for any action by its third-party servicers

Federal Security Controls





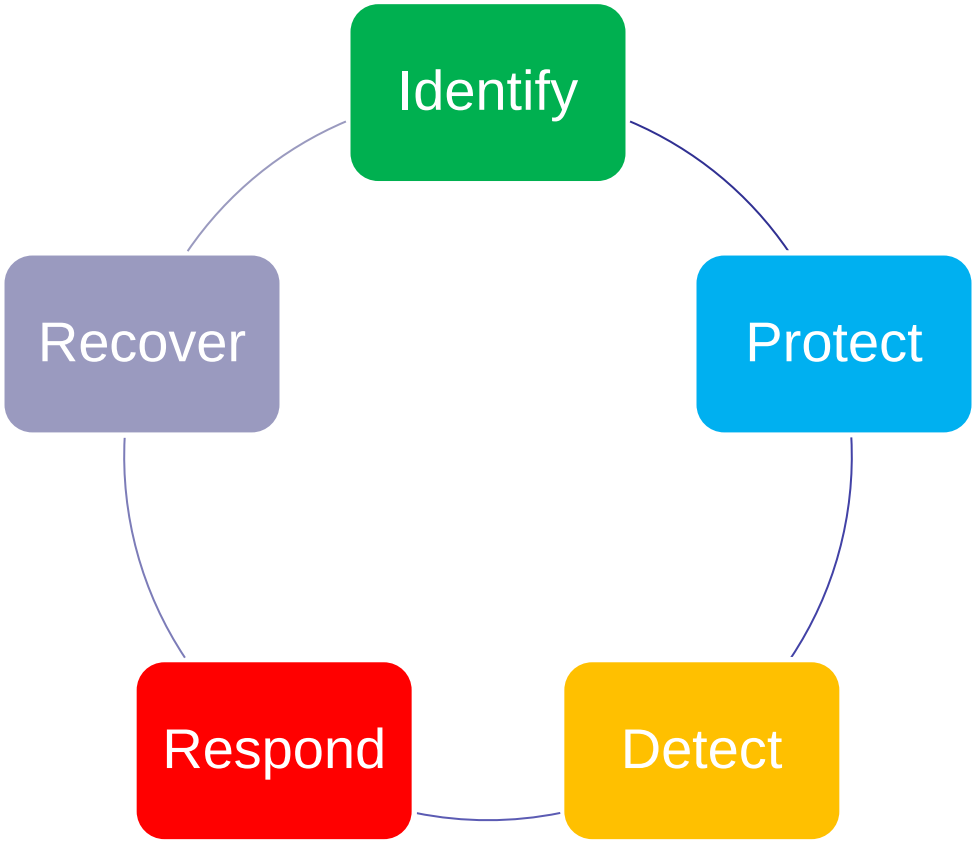
Federal Information Security Management Act (FISMA)

- First enacted in 2002, requires by law that federal data must be secure
- Authorized OMB & NIST to define the standards and guidelines
- Requires periodic reporting of status and audit authorities

FISMA Cyber Security Controls NIST SP 800-53 (rev4)

- What the federal government (and ED/FSA) use to evaluate the security posture of systems and applications that process or store sensitive federal information.
  - Provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations, organizational assets, individuals, and other organizations.
  - Controls are implemented as part of an organization-wide process that manages information security and privacy risk.
  - Controls address a diverse set of security and privacy requirements across the federal government and critical infrastructure, derived from legislation, Executive Orders, policies, directives, regulations, standards, and/or mission/business needs.
  - Controls address security from both a functionality perspective (the strength of security functions and mechanisms provided) and an assurance perspective (the measures of confidence in the implemented security capability).

Cyber Security Framework (FISMA)



1 – Identify risks and risk areas
2 – Protect and implement safeguards
3 – Detect cyber security threats
4 – Respond to a potential incident or threat
5 – Recover and restore capabilities

Protecting Controlled Unclassified Information in NonFederal Information Systems and Organizations NIST SP800-171

- Protecting Controlled Unclassified Information (CUI) in NonFederal environments is of paramount importance to federal agencies due to the potential impact on federal systems
- Focuses on protecting the confidentiality of the data
- Alternatively offers a reduced set of critical controls from FISMA NIST 800-53 for nonfederal entities

Gramm-Leach-Bliley Act (GLBA)

- GLBA requires “financial institutions” to ensure the security and confidentiality of customer personal information
- Colleges and Universities are considered financial institutions under the Act
- All Institutions of Higher Education (IHEs) are required to be compliant with Gramm Leach Bliley Act (GLBA)
- This requirement was recently added to the Program Participation Agreement and is reflected in the *Federal Student Aid Handbook*

GLBA Components

- Safeguards Rule-develop an information security programs:
  - Designate a Security Program Coordinator responsible for coordinating the program
  - Conduct a risk assessment to identify reasonably foreseeable security and privacy risks
  - Establish a System Security Plan that describes how safeguards are employed to control the identified risks; regularly test & monitor the effectiveness of these safeguards

- Privacy Rule
  - Privacy Notice must include how you protect confidentiality of students' data

GLBA - Safeguards Rule

- Assess and address the risks to customer information in all areas of their operation;
- Develop a written information security plan that describes their program to protect customer information;
- Designate one or more employees to coordinate its information security program;
- Identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
- Design and implement a safeguards program, and regularly monitor and test it;
- Select service providers that can maintain appropriate safeguards;
- Evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

GLBA Safeguards–
Employee Management & Training

- Check references or doing background checks before hiring employees
- Ask every new employee to sign an agreement to follow your company's confidentiality and security standards
- Limit access to customer information to employees who have a business reason to see it
- Control access to sensitive information by requiring employees to use "strong" passwords that must be changed on a regular basis
- Use password-activated screen savers to lock employee computers after a period of inactivity
- Develop policies for appropriate use and protection of devices
- Train employees to take basic steps to maintain the security, confidentiality, and integrity of customer information
- Impose disciplinary measures for security policy violations
- Prevent terminated employees from accessing customer information

GLBA – Information Systems

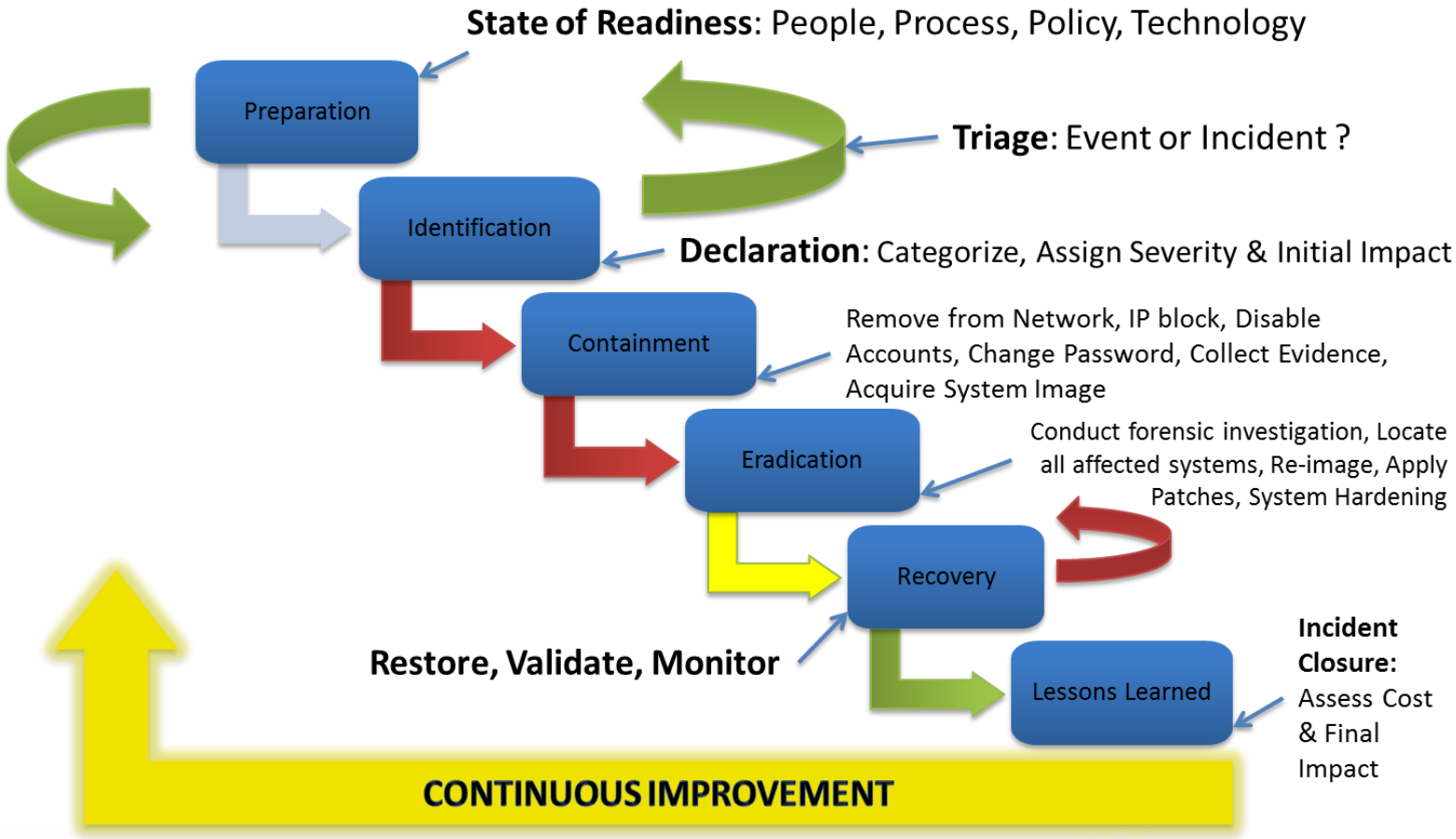
- Know where sensitive customer information is stored and store it securely. Make sure only authorized employees have access
- Take steps to ensure the secure transmission of customer information
- Dispose of customer information in a secure way

GLBA – Safeguards Detecting and Managing System Failures

Deter, detect, and defend against security breaches

- Maintain up-to-date and appropriate programs and controls to prevent unauthorized access to customer information
- Use appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information
- Take steps to preserve the security, confidentiality, and integrity of customer information in the event of a breach
- Consider notifying consumers, law enforcement, and/or businesses in the event of a security breach

6-Step Incident Handling Process



GLBA - Privacy Rule

- Financial institutions must give their customers - and in some cases their consumers - a "clear and conspicuous" written notice describing their privacy policies and practices

- Notice must accurately describe how you collect, disclose, and protect nonpublic information (NPI) about consumers and customers, including former customers

- Notice must provide an accurate description of your current policies and practices with respect to protecting the confidentiality and security

WE have an obligation to the students and parents to protect their Personally Identifiable Information.

FSA systems contain over 130M unique SSNs; the cost of a breach is severe; are you doing all you can do to protect that data?

Breach Information is Public Information

- Privacy Rights Clearing House (Https://privacyrights.org)
- The Open Security Foundation's DataLossDB.org (www.dtatlossdb.org)

Summary - Minimizing Risk

Risk-Based Approach to Security

- Assess the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems.
- Determine the levels of information security appropriate to protect information and information systems.
- Implement policies and procedures to cost-effectively reduce risks to an acceptable level.
- Regularly test and evaluate information security controls and techniques to ensure effective implementation and improvement of such controls and techniques.

Summary - Minimizing Risk

Reduce Your Data Exposure

- Enforce a clean desk policy
- Conduct PII "amnesty" days (shred paper PII/eliminate PII from local and shared drives)
- Protect data at the endpoints
  - Encrypt USB drives
  - Encrypt any hard drives on laptops and any system that store PII
  - Shred paper or store in a locked cabinet
  - Do not leave documents with PII unattended at printers
- Destroy your data securely
- Do not keep records forever
- Limit access to only those with a need to know
- Practice breach *prevention*
  - Analyze breaches from other organizations
  - Learn from their mistakes
  - Adjust your policies and procedures accordingly
- Please - **THINK** before you post/send/tweet!

Summary - Minimizing Risk

Use Strong Passwords

Password strength is related to:

- The number of different characters/numbers available
- How many of those characters/numbers you use (length)
- Whether or not you are using dictionary words or common patterns

Examples:

Password 7 characters (only letters) long = **9 minutes** max to crack

Password 12 characters long (special characters, letters, numbers) = **7,545,667 years** to crack

The Dictionary Attack:

If you use actual words in your password that can be found in a dictionary or use very common patterns, regardless of the length of your password, it can be cracked **in a few seconds to a few minutes**.

- Do these dictionary passwords look familiar?

iloveyou password we1come 123456

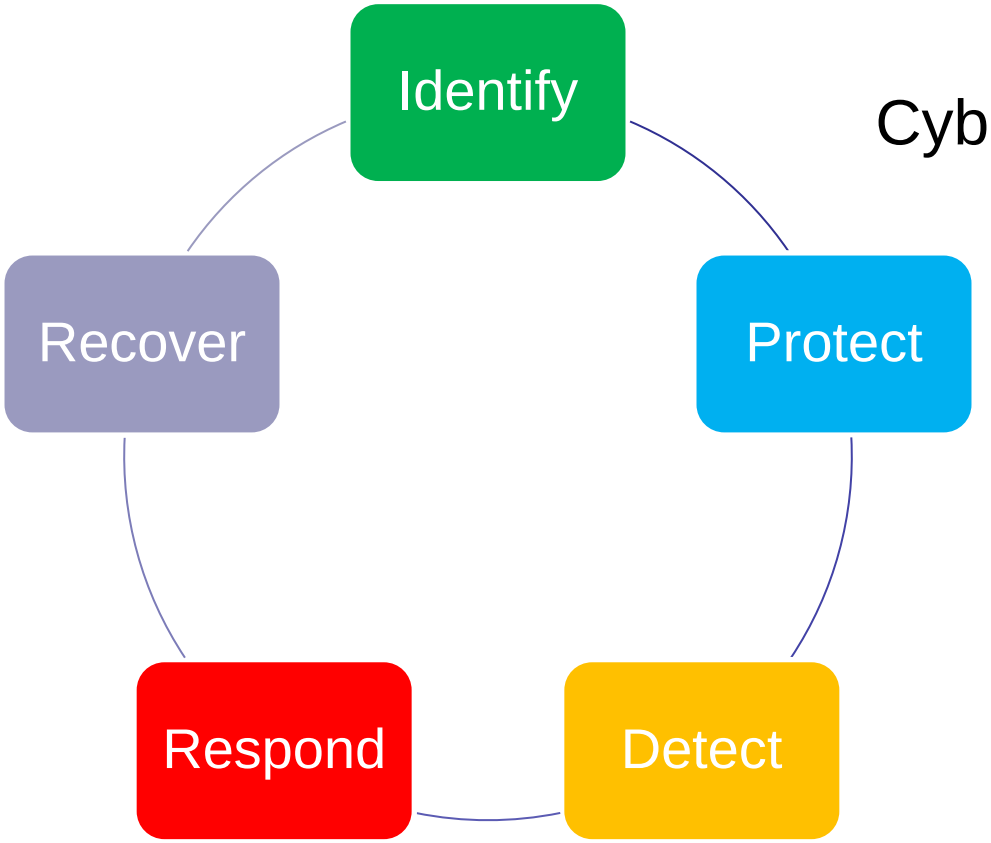
Breach Response

In the event of an actual or suspected breach of FSA applicant PII, the institution must immediately notify FSA at **CPSSAIG@ed.gov**

Follow your local incident/breach response policies.

Requirement set forth in Dear Colleague Letter
Publication Date: July 29, 2015
Subject: Protecting Student Information
DCL ID GEN-15-18

Conclusion



Cyber Security Framework

1 – Identify risks and risk areas
2 – Protect and implement safeguards
3 – Detect cyber security threats
4 – Respond to a potential incident or threat
5 – Recover and restore capabilities

References

- FIPS 199 Categorize Information System
- NIST SP 800-37 Risk Management Framework
- NIST SP 800-53 rev 4 Federal Information Security Management Act
- NIST SP 800-171 Protecting Controlled Unclassified Information in NonFederal Information Systems and Organizations
- Gramm-Leach-Bliley Act (GLBA)

Questions

Dr. Linda R. Wilbanks
FSA CISO
Linda.Wilbanks@ed.gov
202-377-3396