

WELCOME TO #WCETWEBCAST

February 13, 2019

The webcast will begin shortly.

There is no audio being broadcast at this time.

An archive of this webcast will be available on the SAN website next week.





DATA PROTECTION AND PRIVACY WHAT INSTITUTION STAFF NEEDS TO KNOW!

February 13, 2019



WELCOME!

Use the question box for questions and information exchange.

Archive, PowerPoint, and Resources will be available next week.

PowerPoint can be downloaded in the handouts pane.

Follow the Twitter feed: #WCETWebcast.



Megan Raymond
Assistant Director, Programs & Sponsorship
WCET

mraymond@wiche.edu

@meraymond





MODERATOR

Name: Cheryl Dowd

Title: Director, State Authorization Network (SAN)

Org: WCET

QUESTIONS FROM THE AUDIENCE

If you have a question during the presentation, please add your questions to the question box.

We will monitor the question box and have time for Q&A at the end of the presentation.



PRESENTERS



Baron Rodriguez
Data Privacy Expert
Owner/CEO, Noble Privacy Solutions, LLC



Tiina K.O. Rodrigue
Cybersecurity Subject Matter Expert

AGENDA

- DATA PROTECTIONS AND PRIVACY: WHAT INSTITUTION STAFF NEEDS TO KNOW.
- GLBA – WHAT SAFEGUARD REQUIREMENTS APPLY?
- GLBA - NIST FRAMEWORKS – WHAT SHOULD I USE?



DATA PRIVACY & SECURITY: ARE THESE SYNONYMOUS?

Privacy:

- *Relates to rights you or others have to control personal information and how it's used*



Data Security:

- *The “how” information (personal or other types) are protected*



KEY DATA PRIVACY EVENTS/DRIVERS

- ❑ FERPA – Attempts at modernization.
- ❑ Consumer Privacy Bill of Rights – Start/Stop – industry and advocates push back.
- ❑ GDPR – May 25th, - Consumer Protection/Non-Sectoral – Europe.
- ❑ CACPA – First comprehensive state-based consumer privacy law.
- ❑ 12 States pass data breach, consumer protection laws: AL, CA, CO, IA, LA, NE, OR, SC, SD, VT, VA.
- ❑ Google, AT&T, Amazon, other tech giants release “Framework for New Privacy Laws”.



CONSUMER BREACH DRIVERS

- Facebook/Cambridge Analytica
- Healthcare
- Financial Breaches
- Ransomware
- Phishing



COMING SOON? PROPOSED NATIONAL PRIVACY FRAMEWORK

- ✓ Collect and use personal information responsibly.
- ✓ Mandate transparency and help individuals be informed.
- ✓ Place reasonable limitations on the manner and means of collecting, using, and disclosing PII.
- ✓ Maintain the quality of personal information.
- ✓ Make it practical for individuals to control the use of PII.
- ✓ Give individuals ability to access, correct, delete and download PII about them.
- ✓ Include requirements to secure personal information.

Source: https://services.google.com/fh/files/blogs/google_framework_responsible_data_protection_regulation.pdf

PART 2: PROPOSED NATIONAL PRIVACY FRAMEWORK

- ✓ Hold organizations accountable for compliance.
- ✓ Focus on risk of harm to individuals and communities.
- ✓ Distinguish direct consumer services from enterprise services.
- ✓ Define personal information flexibility to ensure proper incentives & handling.
- ✓ Design regulations to improve the ecosystem and accommodate changes in technology and norms.
- ✓ Apply geographic scope that accords with international norms.
- ✓ Encourage global interoperability.



CALIFORNIA CONSUMER PRIVACY ACT

CURRENTLY Applies to

- **For profits** that collect personal information, determine the means/purpose for processing that info, do business in CA and have one of the following:
 - Gross revenue >\$25M;
 - Buy, sell, receive or share personal information for commercial services; or
 - Derive >50% of its annual revenue from selling personal information.
- Service providers (think contractors, cloud services, “free aps”).
- Third parties – Similar to above, but could include entities that received shared data.

WHAT'S COVERED UNDER CACPA?

- ✓ Collection of personal information.
- ✓ Sale of personal information.
- ✓ Disclosure of personal information.



CALIFORNIA CONSUMER PRIVACY ACT

- ❑ Goes into effect 2020, covers residents of California.
- ❑ Likely will be several modifications/amendments before 2020.



POTENTIAL SCENARIOS FOR SCHOOLS

- Study-Abroad Programs and Overseas Offices
- Distance Learning
- Admissions Office
- Alumni and Development Office
- Registrar/Student Records
- Online Institutions
- Research Centers
- Vendors



WHAT STUDENT CAN DO:

- Withdraw consent for processing.
- Request a copy of all of their data.
- Request the ability to move their data to a different organization.
- Request that you delete information they consider no longer relevant.
- Object to automated decision-making processes, including profiling.



WHAT REGULATORS CAN DO:

- Ask for records (proof) of processing activities and proof of steps taken to comply with the GDPR .
- Impose temporary data processing bans, require data breach notification, or order erasure of personal data.
- Suspend cross-border data flows.
- Enforce penalties of up to 20 million Euro or 4 percent of annual revenues for non-compliance.

CYBERSECURITY REQUIREMENTS

JUST LIKE FERPA: GDPR requires organizations to “Implement appropriate technical and organizational measures” (based on risks to rights and freedoms of individuals).

- Pseudonymization and encryption of personal data.
- Ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems/services.
- Ability to restore and provide access to personal data in a timely manner.
- Process for regularly testing, assessing, and evaluating the effectiveness of your privacy and cybersecurity measures/systems.



NOTICE REQUIREMENTS

Transparency requirement of GDPR:

- Must update your policies and provide students with information including, purposes for collecting their personal data, your retention periods and who it will be shared with. (including Alumni, third parties, and International data transfers).
- Information must be concise, transparent, accessible and easy to understand.
- Regularly review and update this notice on a regular basis.
- See the checklist located here for more specifics on what needs to be in your notice: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/> .



DO YOU NEED A DATA PROTECTION OFFICER? (DPO)

Does your organization regularly process personal information on data subjects on a large scale?

Do you process data consisting of special categories on a large scale?

Even if not, it is a best practice to identify a single point of contact in the event of questions regarding data protections or in the event of a breach.

GLBA – WHAT SAFEGUARD REQUIREMENTS APPLY?

February 13, 2019



GRAMM LEACH BLILEY ACT - 2002

Written to protect consumer financial data under the auspices of FTC.

Why does it apply to Higher Ed?

- FTC ruled that Higher Ed Institutions that underwrite/loan money/ have student accounts fall under GLBA.
- Department of Education further reinforced GLBA requirements:
 - Program Participation Agreement – must adhere to GLBA Safeguard Standards;
 - Student Aid Internet Gateway Agreement – adhere to GLBA and report breaches immediately; and
 - Pattern and Practice:
 1. HEA - Administrative Capability.
 2. FAFSA data is Federal Data – must be protected.

GLBA - SAFEGUARDS

GLBA Safeguards are clear, but not standards. Each institution must:

- Develop, implement, & maintain documented data security (info-security) program
 - A policy is not a program – the effort has to have enforcement and funding
 - Must be sufficient to address the risks and controls
- Designate an employee(s) to coordinate the program
 - Can't be outsourced – must be an official employee responsible
 - Can be a secondary duty – must perform within the parameters
 - Best practice – trained, information security professional



GLBA SAFEGUARDS - CONT

- Identify reasonably foreseeable internal and external risks to data security via formal, documented risk assessments.
 - Best practice – internal self checks, independent assessments.
 - How often are you doing risk assessments, corrections?
- Control the risks identified, by designing and implementing information safeguards and regularly test /monitor their effectiveness.
 - Controls are physical, technical, and administrative.
 - What is your testing schedule?
 - How do you know that your controls work? How do you monitor?
 - What is your response plan when there is a potential incident or breach?



GLBA SAFEGUARDS

Oversee service providers –

- Institutions remain responsible for data safeguards regardless of who is hired
- Service providers are anyone who has access to the data, to include:
 - Cloud providers;
 - IT Professionals / Contractors;
 - Data Destruction Services; and
 - 3rd-Party Servicers.
- Take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the FSA, student, & school (customer) information at issue.
 - Data should remain as safe with the service provider, as if data never left FSA, institution.
- Require your service providers by contract to implement and maintain all GLBA safeguards.
 - Review contracts to ensure breaches are reported immediately.
 - Work with legal to make contract language binding, enforceable, measured.



GLBA SAFEGUARDS

Evaluate & adjust school's info-sec program in light of:

- Results of the required testing /monitoring.
 - This should be documented and regularly updated.
 - Cyberthreats are dynamic – out of date programs won't protect anyone.
- Any material changes to your operations or business arrangements.
 - Staffing changes – Executives
 - Mergers, acquisitions, divestures
- Any other circumstances that you know may have a material impact on your information security program.
 - Any time you have new forms, new data – this needs to be considered.



GLBA RISK ASSESSMENTS

- 1) Employee training and management:
 - Do you have up-to-date GLBA/Data security policies?
 - Do you have employee GLBA/Data security training? Are your managers trained to handle misuse?
 - How are your managers enforcing safe data policies? Can you prove it?
- 2) Information systems, including network and software design, as well as information processing, storage, transmission, and disposal:
 - How often do you assess all of your systems/code, if ever? Is anything obsolete?
 - If your data is a river, how shored is everywhere it flows? Best practice – 2 safeguards for each vector
- 3) Detecting, preventing and responding to attacks, intrusions, or other systems failures:
 - How do you detect that you are under attack, or worse, hosting attacks? How do you prevent attacks?
 - What are your potential human system failures – insider threat or unauthorized use/access?
 - What is your notification, communication, and escalation plan within the program?



WHAT IS A GLBA BREACH?

- Per GLBA, a breach is *any unauthorized disclosure, misuse, alteration, destruction or other compromise of information – and this is what your risk assessment must consider. This is in agreement with GDPR. Better to report suspicions, don't wait.*
- Administrative, technical, and physical safeguards prevent breaches:
 - 1) Ensure the security & confidentiality of customer information.
 - 2) Protect against any anticipated threats or hazards to the security or integrity of such records.
 - 3) Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.



GLBA - NIST FRAMEWORKS – WHAT SHOULD I USE?

February 13, 2019



WHAT IS NIST? FRAMEWORKS?

- NIST is the National Institute of Standards and Technology.
- Run by the Department of Commerce – mandated to create and run.
 - Federal Information Processing Standards ([FIPS](#))
 - Special Publications (SP) on Data Security ([800 Series](#))
 - [Encryption Strength Tests](#) to ensure sufficiency
- Have a framework for almost every need – data security.
 - Creates best practices and reference for training, frequency.



WHICH FRAMEWORKS SHOULD I USE?

The following are not requirements but are sufficient to prove GLBA compliance:

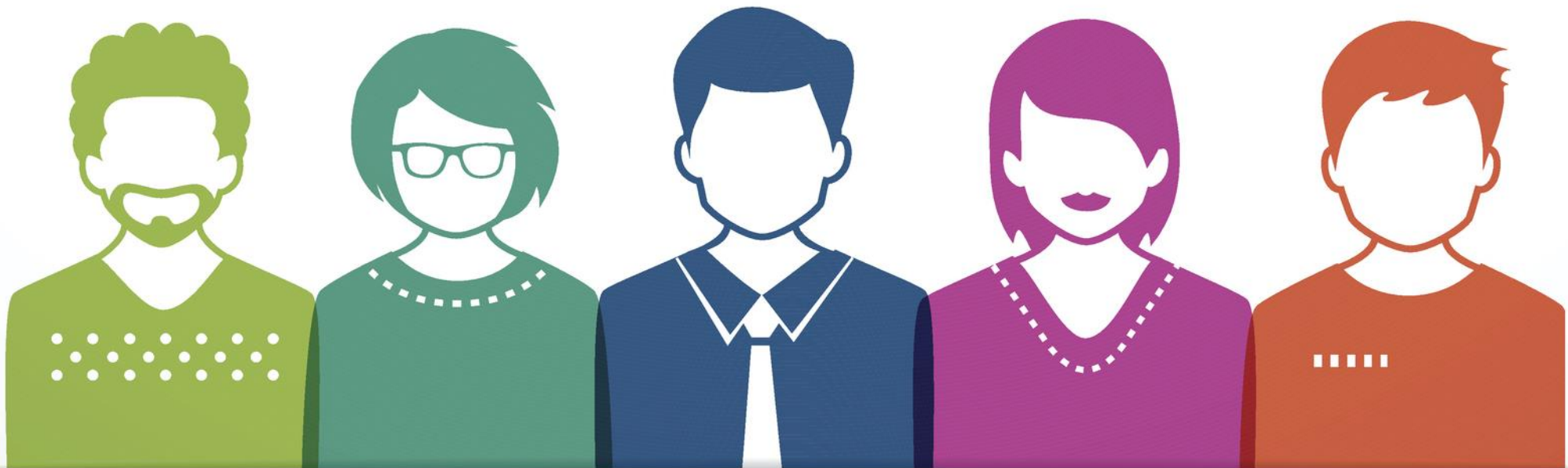
- Data Security for Non-Federal Systems Framework [800-171](#) recommended by [16-12](#)
 - How to do Data-Security Assessments [800-171A](#)
- Role-Based Data Security Training Framework (NICE) – [800-181](#)
 - Free NICE Data-Security Training - [NICCS](#)
- Risk Management Framework (RMF) – [800-37](#)
 - How to conduct Risk Assessments – [800-30](#)
- Data-Security Monitoring – [800-137](#)

TODAY'S TO-DOS (IF NOT A YES, THEN DO)

1. Find your data security program documentation – less than 3 years old? More than a policy?
2. Does your data security program have a current, documented, trained employee with his/her contact information - one who is actively managing/coordinating the program?
3. What is the information risk assessment/ data-security testing schedule in place?
4. Are the tests and results documented based on that schedule and any findings being fixed?
5. Is your information security policy/program/schedule/contact information on your consumer information and compliance website so that you can easily find/maintain it?
6. Is each employee trained for his/her/their data security role? Are you managing and enforcing?
7. Is your entire executive team prepared to respond immediately & appropriately when a breach happens? Have you run any tabletops to test this?



QUESTIONS FROM THE AUDIENCE



CONTACT INFORMATION

You can contact both presenters at the following location:

Tiina Rodrigue & Baron Rodriguez:

baron@nobleprivacysolutions.com

www.nobleprivacysolutions.com



LEARN MORE AND STAY CONNECTED

Visit WCET's website to learn about our
Focus Areas, Initiatives, Events,
Membership and Sponsorship:

<http://wcet.wiche.edu/>

Join WCET: learn more about the benefits
of joining our national community:

<http://wcet.wiche.edu/join-wcet>

Visit the SAN website to learn more
about our topic areas and research!

<http://wcetSAN.wiche.edu>

Join SAN: learn more about benefits,
services and events:

<http://wcetSAN.wiche.edu/membership>

Focus Areas ▾

Initiatives ▾

Events ▾

Get Involved ▾



LEARN MORE AND STAY CONNECTED

WCET/SAN Basics Workshop
March 6 -7, 2019
Arlington, VA (Wash. DC Metro Area)

Sold Out

WCET/SAN Advanced Topics Workshop
Fall 2019

Stay tuned as it will be announced soon!

NASASPS (state regulators) Annual Conference
SAN member sessions & collaborative agenda
April 14-17, 2019
Jacksonville, FL

Hyatt Regency Jacksonville Riverfront

[Register now!](#)

*code required for SAN Member rate



ADDITIONAL INFORMATION AND RESOURCES

Access to the resources discussed during this webcast, including the archive, will be available next week for SAN members on the SAN Website.

[Resources: Past Webinars](#)

THANK YOU SUPPORTING
MEMBERS FOR YOUR
COMMITMENT TO WCET
AND E-LEARNING

*Colorado State
University*


*Michigan State
University*

*University of
Missouri -
Columbia/Mizzou
Online*


*University of North
Texas*




THANK YOU WCET ANNUAL SPONSORS




WILEY
EDUCATION SERVICES




BARNES & NOBLE EDUCATION **LoudCloud** **LEAR N**
Pearson **CENGAGE** **Blackboard**
THE CHRONICLE
of Higher Education*



VitalSource



Realizeit **PeopleGrove** **wyzant**
Powering intelligent pathways to mastery



NameCoach **iDesign**
hear the name, say it right

D2L **intellus LEARNING** **LearningMate** **@-LITERATE**
DESIRE2LEARN

YOU
at COLLEGE

