



Future of Privacy Forum Higher Education Working Group

GLBA Safeguards Rule

*Dean Forbes
Counsel*

September 29, 2017

Agenda

- **Introductions**
- **Department of Education Publications on Protecting Student Information**
- **GLBA Privacy and Safeguards Rules**
- **FTC Orders and NIST**
- **Questions and Discussion**

Presenter



Dean C. Forbes

Counsel

Washington, D.C.

1.202.736.8165

dforbes@sidley.com

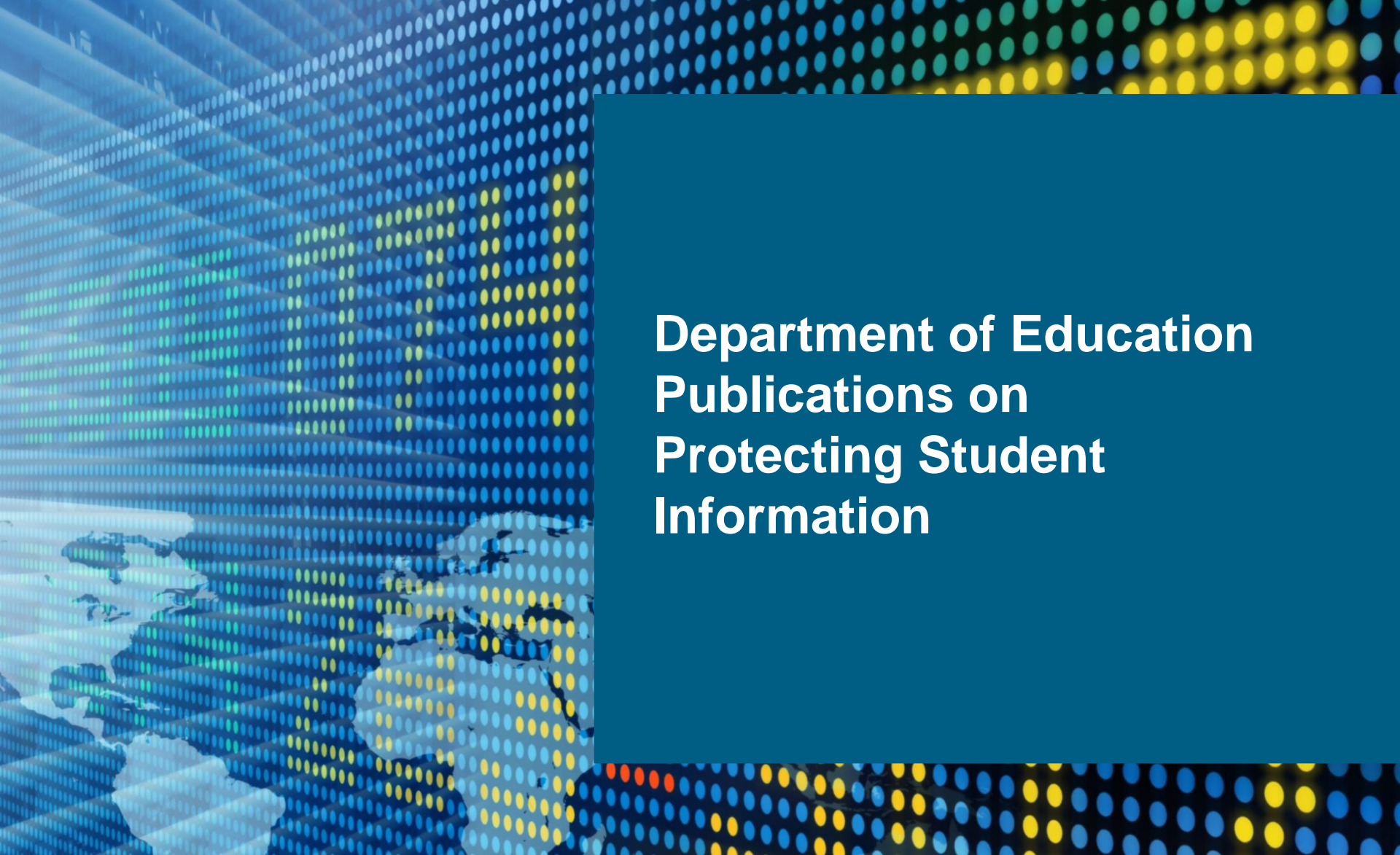
Education: University of Virginia School of Law (J.D., 1991); Brown University (A.B., 1987)

Practice Groups: Privacy & Cybersecurity, and Healthcare

DEAN is an accomplished global privacy, cybersecurity, and compliance legal adviser. He has advised and represented clients in a variety of industries, including health care, financial services, high tech, energy, and education, on matters related to privacy strategy, security, data governance and use, and consumer protection.

Dean is widely known for his work on cases of first impression—including landmark FTC privacy and information security matters, Geocities (1998) and Eli Lilly (2002)—and for designing, developing and executing global privacy programs that manage privacy risks and protect companies and their stakeholders.

- Former Lead, Commercial Privacy Practice, Booz Allen Hamilton
 - Former Global Privacy Officer, Schering-Plough (also held senior roles at Merck and Johnson & Johnson)
 - Former Sr. Staff Attorney, Federal Trade Commission, Bureau of Consumer Protection
 - Former Board Member, International Association of Privacy Professionals (IAPP)
-



Department of Education Publications on Protecting Student Information

Department of Education

Publications on Protecting Student Information

- Federal Student Aid (FSA), Department of Education Publications:
 - DCL ID: GEN-15-18 (July 29, 2015)
 - DCL ID: GEN-16-12 (July 1, 2016)
- Subject: Protecting Student Information
- Reminders to institutions of higher education and their 3rd party service providers of continuing obligations to protect data used in administering Title IV Federal student financial aid programs
- To support Student Aid Internet Gateway (SAIG) Enrollment Agreement entered into by each Title IV participating institution, FSA has strongly encouraged institutions to follow industry standards and best practices in managing information and information systems, and in securing PII
- In addition, FSA requires institutions to comply with the Gramm-Leach-Bliley Act (GLBA)
 - Under Title V, financial services organizations, including institutions of higher education, are required to ensure the security and confidentiality of customer records and information.
 - Requirement recently added to Program Participation Agreement (PPA); is reflected in the Federal Student Aid Handbook
- The Department of Education plans to audit educational institutions for GLBA compliance
 - More info here: <https://ifap.ed.gov/dpccletters/GEN1612.html>
- The Department strongly encourages institutions to review and understand the standards defined in NIST SP 800-171

Educational Institution Gramm-Leach-Bliley Act (GLBA) Safeguards Rule Compliance – Information Security Program

- Each educational institution's PPA includes provision requiring GLBA compliance
- Under the GLBA, financial services organizations, which include postsecondary educational institutions, are required to ensure the security and confidentiality of student financial aid records and information.
- Among other things, the GLBA requires institutions to:
 - Develop, implement, and maintain a written information security program
 - Designate the employee(s) responsible for coordinating the information security program
 - Identify and assess risks to customer information
 - Design and implement an information safeguards program
 - Select appropriate service providers capable of maintaining appropriate safeguards, and
 - Periodically evaluate and update their security program
- Educational Institution Presidents and CIOs should have, at a minimum:
 - evaluated and documented their current security posture against GLBA's requirements
 - taken immediate action to remediate any identified deficiencies
- Department of Education:
 - incorporating GLBA security controls into Annual Audit Guide, to assess and confirm institutions' GLBA compliance
 - will require examination of evidence of GLBA compliance as part of institutions' annual student aid compliance audit.



The GLBA Privacy and Safeguards Rules

GLBA

- The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, requires financial institutions to:
 - explain their information-sharing practices to customers
 - limit sharing and disclosure of financial data with third parties
 - safeguard sensitive data

Gramm-Leach-Bliley Act

- Requirement for initial and annual privacy notices
- Required options for information sharing
 - Some sharing does not require opt-out
 - “As permitted by law”
 - Own advertising
 - Joint marketing
 - Affiliate sharing (regulated by the FCRA)
 - Sharing transaction & experience information
 - Sharing creditworthiness information
 - Sharing for affiliates’ marketing purposes
 - Sharing with non-affiliates
- New exception for annual notice requirement
 - Applies only if the financial institution has a “no sharing” policy
 - Applies only if the privacy policy has not changed from the prior communication

Safeguards

- Title V of the GLBA sets out a number of mechanisms to protect the privacy and security of non-public personal information collected by financial institutions in connection with the provision of a financial product or service. Requires financial institutions to:
 - provide notices of policies and practices regarding disclosure of personal information
 - prohibit the disclosure of such data to unaffiliated third parties unless consumers are provided the right to “opt out” of such disclosure or unless other exceptions apply, and
 - establish safeguards to protect the security of personal information
- To whom does the safeguards rule apply?
 - Applies to “financial institutions” (see section 313.3(k) on applicability)
 - All businesses, regardless of size, that are “significantly engaged” in providing financial products or services
- What steps should your organization take to comply?
- Securing personal information
 - Reasonable and appropriate security measures

The Safeguards Rule requires

- The Safeguards Rule requires companies to:
- Assess and address risks to customer information
 - in all areas of their operations, including 3 areas important to information security:
 - Employee Management and Training
 - Information Systems, and
 - Detecting and Managing System Failures
- Determine what information they are collecting and storing, and whether they have a business need to do so

The Safeguards Rule requires

- GLBA Safeguards Rule requires companies to:
 - develop written information security plan
 - describes program to protect customer information
 - appropriate to company's size and complexity
 - nature and scope of its activities
 - sensitivity of the customer information it handles.
- As part of its plan, each company must:
- 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, make sure your contract requires them to maintain safeguards, and oversee their handling of customer information, and
- 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

Examples of Reasonable Security Measures

- Checking references and background checks of employees with access to customer PII
- New hires agree to follow security measures
- Limit access based on role
- Access controls, including strong passwords
- Password activated screen savers
- Policies and procedures, including for mobile devices
- Training
- Remind employees of obligations
- Policy for telecommuters
- Imposing disciplinary measures
- No access for terminated employees
- Data asset inventory / data element inventory
- Secure data storage, transmission, and destruction
- Keep security controls up to date



FTC Orders and NIST

FTC Orders: Comprehensive Information Security Programs

- FTC security cases typically require respondents to establish and maintain a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers, including the security, confidentiality, and integrity of personal information accessible to end users.
- The security program must contain administrative, technical, and physical safeguards appropriate to each respondent's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information collected from or about consumers. Specifically, the orders require respondents to:
 - Designate an employee or employees to coordinate and be accountable for the information security program.
 - Identify material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.
 - Design and implement reasonable safeguards to control the risks identified through risk assessment, and regularly test or monitor the effectiveness of the safeguards' key controls, systems, and procedures.
 - Develop and use reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondents, and require service providers by contract to implement and maintain appropriate safeguards.
 - Evaluate and adjust the information security program in light of the results of the testing and monitoring, any material changes to the company's operations or business arrangements, or any other circumstances that they know or have reason to know may have a material impact on the effectiveness of their information security program.

Executive Order 13636 / NIST Cybersecurity Framework

- *Executive Order 13636 : Improving Critical Infrastructure Cybersecurity (2/12/13)*
 - “It is the policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties”
- NIST directed to work with stakeholders to develop voluntary framework for reducing cyber risks to critical infrastructure
- The Framework’s compilation of practices is referred to as the “Core,” which comprises 5 concurrent and continuous functions for managing cybersecurity risk:
 - Identify
 - Protect
 - Detect
 - Respond
 - Recover

FTC Enforcement Aligns with NIST Framework

- **Exemplary FTC enforcement actions illustrate where companies allegedly could have better protected consumers' personal information, if they had followed the NIST Framework's Core Functions.**
- **Identify.**
 - Certain FTC cases have alleged that certain companies had failed to take appropriate action to assess security risks and develop plans to address them (i.e., take reasonable steps to identify vulnerabilities and threats to determine the risk to consumers' personal information)
 - *CVS Caremark Corporation and Petco Animal Supplies, Inc.*
 - FTC alleged that these companies failed to implement policies/procedures to safeguard consumers' information
 - Aligns with NIST Framework guidance on establishing an organizational information security policy
 - *HTC America, Inc. and TRENDnet, Inc.*
 - FTC alleged that these companies did not have a process for receiving, addressing, or monitoring reports about security vulnerabilities
 - Aligns with Framework guidance that companies should consider having a method for receiving threat and vulnerability information from information-sharing forums and sources

FTC Enforcement Aligns with NIST Framework Core Functions

- **Protect.**

- Certain FTC cases have alleged company failures to develop and implement reasonable information security safeguards and practices
- *Twitter, Inc.*
 - FTC alleged that Twitter gave most of its employees administrative access to its system, increasing the risk that a compromise of any of its employees' credentials could result in a serious breach
 - Aligns with Framework's guidance about managing access permissions, incorporating the principles of least privilege and separation of duties
- *Accretive Health, Inc. and Cbr Systems, Inc.*
 - FTC alleged that an employee transported a laptop/portable media with personal information in a manner that made it vulnerable to theft or other misappropriation – in both cases, the laptops and the portable media were stolen, exposing personal information of thousands of individuals
 - Aligns with Framework's guidance on protecting data-in-transit and formally managing assets throughout removal, transfers, and disposition

FTC Enforcement Aligns with NIST Framework Core Functions

- **Detect.**

- Certain FTC cases have alleged that companies have not had appropriate processes in place to monitor activity on their networks and detect intrusions – to reduce the risk of a data compromise or the breadth of compromise
- *Dave & Buster's, Inc.*
 - FTC alleged that Dave and Buster's didn't use an intrusion detection system and didn't monitor system logs for suspicious activity
- *Franklin's Budget Car Sales, Inc.*
 - FTC alleged that Franklin's didn't inspect outgoing Internet transmissions to identify unauthorized disclosures of personal information
 - Both FTC cases align with the Framework's guidance concerning monitoring networks for potential cybersecurity events, and for unauthorized personnel, connections, devices, and software

FTC Enforcement Aligns with NIST Framework Core Functions

- **Respond.**

- Certain FTC cases have challenged certain companies' failures to execute and maintain reasonable response processes and procedures, including breach detection and also taking appropriate steps when a breach occurs (i.e., contain events and communicate their occurrence with the appropriate parties)
- *Wyndham Worldwide Corporation*
 - FTC alleged that Wyndham failed to follow proper incident response procedures, including failing to monitor its computer network for malware used in a previous intrusion, and that, as a result, intruders were able to gain access to the company's computer network on 3 separate occasions in a 21-month period, leading to compromise of 619,000+ payment card account numbers and \$10.6+ million in fraud loss
- *ASUSTeK Computer, Inc.*
 - FTC alleged that: ASUSTeK learned of several vulnerabilities affecting its routers, that despite this knowledge, failed to provide adequate notice to consumers about these risks, the steps consumers could have taken to mitigate them, and the availability of software updates that would correct/mitigate the vulnerabilities, and that, as a result, hackers located consumers' routers and exploited the vulnerabilities gaining unauthorized access to 12,900+ connected storage devices
 - Aligns with Framework guidance on voluntarily sharing information with external stakeholders to achieve broader awareness of cybersecurity threats

FTC Enforcement Aligns with NIST Framework Core Functions

- **Recover.**

- The Recover function supports a return to normal operations after a cybersecurity event. Certain FTC orders demonstrate the importance of this function, emphasizing how consumer interests should factor into a company's recovery plan.

- *Oracle Corporation*

- FTC order required Oracle to provide broad notice to its users about its settlement with the FTC , and how to address Java vulnerabilities.
- FTC ordered Oracle communicate to users through its website and social media, and also by working with external parties, such as antivirus vendors and browsers
- Aligns with Framework's guidance that companies should consider communicating recovery activities with internal and external parties, including coordinating centers, Internet Service Providers, victims, and vendors

- For more information, see:

- <https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc>

Questions & Discussion



Dean Forbes: dforbes@sidley.com

Practice Site: www.Sidley.com/en/services/privacy-and-cybersecurity

Blog: www.DataMatters.Sidley.com

This presentation has been prepared by Sidley Austin LLP as of September 26, 2017 for educational and informational purposes only. It does not constitute legal advice. This information is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this without seeking personalized advice from professional advisers.

BEIJING BOSTON BRUSSELS CHICAGO DALLAS FRANKFURT GENEVA HONG KONG HOUSTON LONDON LOS ANGELES NEW YORK PALO ALTO SAN FRANCISCO SHANGHAI SINGAPORE SYDNEY TOKYO WASHINGTON, D.C.



Sidley Austin LLP, a Delaware limited liability partnership which operates at the firm's offices other than Chicago, New York, Los Angeles, San Francisco, Palo Alto, Dallas, London, Hong Kong, Houston, Singapore and Sydney, is affiliated with other partnerships, including Sidley Austin LLP, an Illinois limited liability partnership (Chicago); Sidley Austin (NY) LLP, a Delaware limited liability partnership (New York); Sidley Austin (CA) LLP, a Delaware limited liability partnership (Los Angeles, San Francisco, Palo Alto); Sidley Austin (TX) LLP, a Delaware limited liability partnership (Dallas, Houston); Sidley Austin LLP, a separate Delaware limited liability partnership (London); Sidley Austin LLP, a separate Delaware limited liability partnership (Singapore); Sidley Austin, a New York general partnership (Hong Kong); Sidley Austin, a Delaware general partnership of registered foreign lawyers restricted to practicing foreign law (Sydney); and Sidley Austin Nishikawa Foreign Law Joint Enterprise (Tokyo). The affiliated partnerships are referred to herein collectively as Sidley Austin, Sidley, or the firm.

For purposes of compliance with New York State Bar rules, Sidley Austin LLP's headquarters are 787 Seventh Avenue, New York, NY 10019, 212.839.5300 and One South Dearborn, Chicago, IL 60603, 312.853.7000.

1,900 LAWYERS and **20 OFFICES**
located in commercial, financial
and regulatory centers
around the world



Beijing
Boston
Brussels
Century City

Chicago
Dallas
Geneva
Hong Kong

Houston
London
Los Angeles
Munich

New York
Palo Alto
San Francisco
Shanghai

Singapore
Sydney
Tokyo
Washington, D.C.

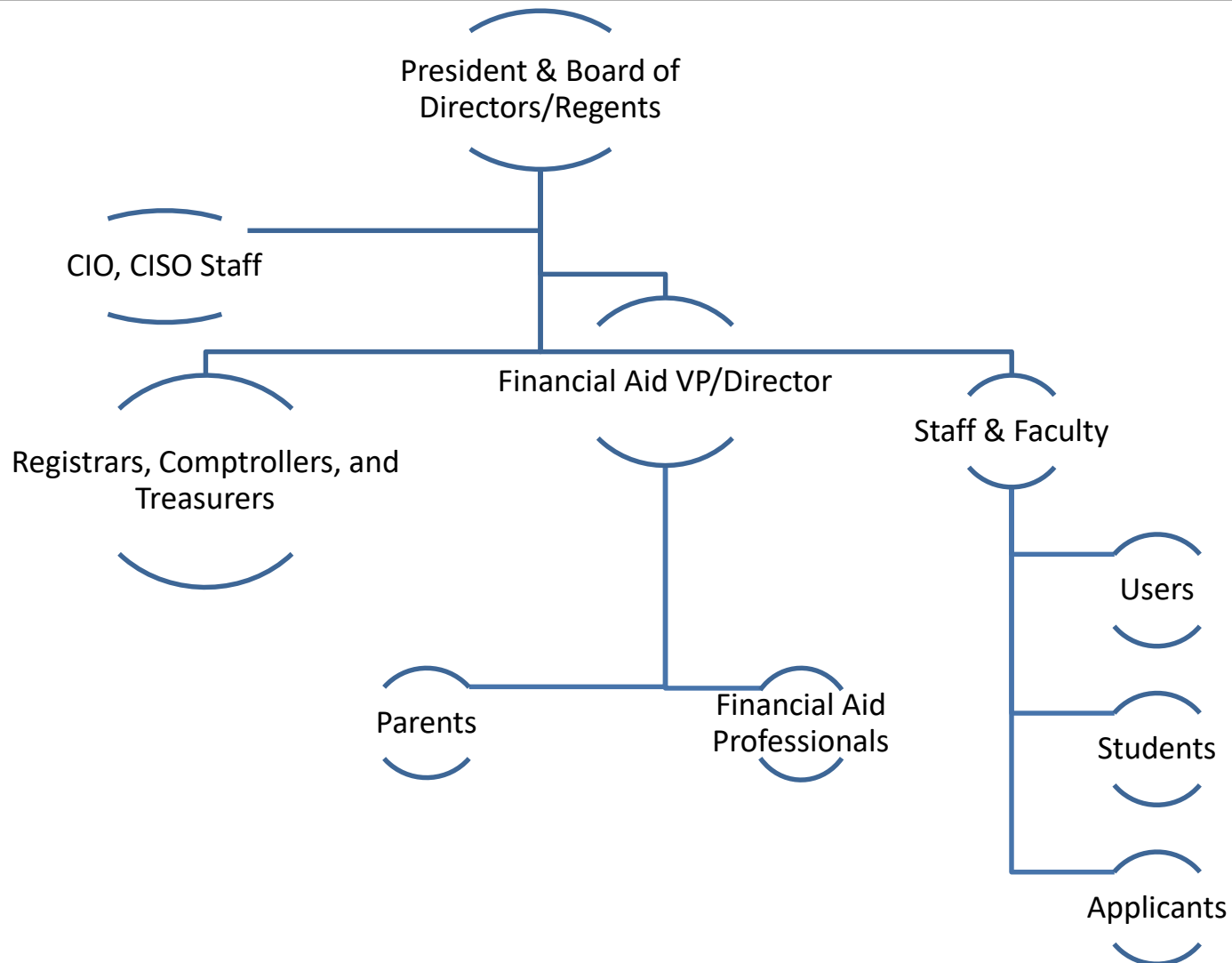
Post-Secondary Institution Data-Security Overview and Requirements

Tiina K.O. Rodrigue, EdDc, CISSP, CISM, PMP, CSM,
CEA, ITIL, ISC2 Compliance Mapper, A+
Senior Advisor – Cybersecurity - 2017

Agenda

- Who needs to worry about data security?
- Why do I need to worry about data security?
- What are the data security requirements?
- What is a breach?
- When do I report a breach?
- How do I report a breach?
- How can you help me with data security?
- What are my next steps?

Who needs to worry about data security?



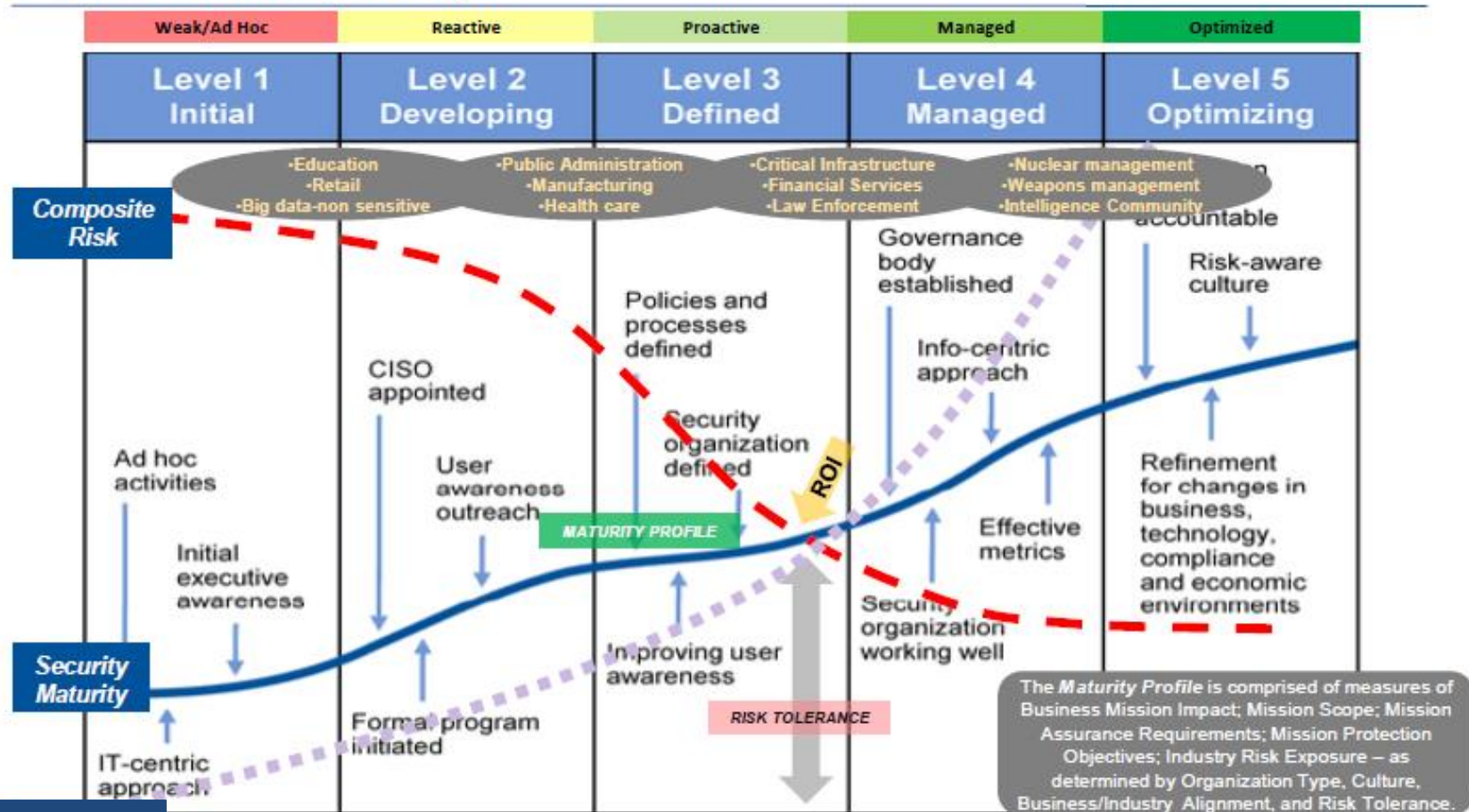
Why do I need to worry about data security?

Results Introduction

Gartner

A Primer for Security Maturity

Gartner Research indicates that it typically requires 3 – 4+ years for a government organization to incrementally change maturity levels within their environments (e.g., level 2 to level 3)



Why do I need to worry about data security?

Educational institutions are specifically being targeted because of the current state of ad-hoc security coupled with the educational environment being a rich trove of emails, information and research.



Why do I need to worry about data security?

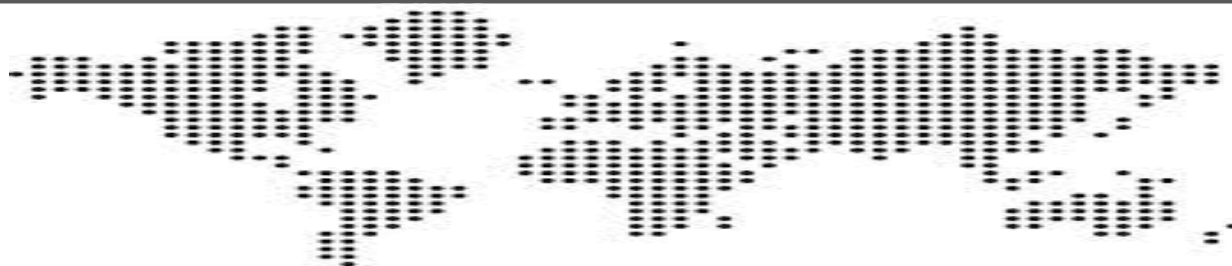
Starting in FY18, GLBA information security safeguards will be audited to ensure administrative capability. Draft audit language:

Audit Objectives – Determine whether the IHE designated an individual to coordinate the information security program; performed a risk assessment that addresses the three areas noted in 16 CFR 314.4 (b) and documented safeguards for identified risks.

Suggested Audit Procedures

- a. Verify that the IHE has designated an individual to coordinate the information security program.
- b. Obtain the IHE risk assessment and verify that it addresses the three required areas noted in 16 CFR 314.4 (b).
- c. Obtain the documentation created by the IHE that aligns each safeguard with each risk identified from step b above, verifying that the IHE has identified a safeguard for each risk.

What are the data security requirements?



- Title IV schools are financial institutions per *Gramm-Leach-Bliley Act* (GLBA, 2002)
- Per FSA PPA & SAIG agreements, these schools must have GLBA safeguards in place. Schools without GLBA safeguards may be found administratively incapable (unable to properly administer Title IV funds).
- GLBA Safeguards are:
 - Develop, implement, & maintain documented data security (info-sec) program
 - Designate an employee(s) to coordinate the program

What are the data security requirements? cont'd

- Identify reasonably foreseeable internal and external risks to data security via formal, documented risk assessments of:
 - 1) Employee training and management
 - 2) Information systems, including network and software design, as well as information processing, storage, transmission, and disposal
 - 3) Detecting, preventing and responding to attacks, intrusions, or other systems failures
- Control the risks identified, by designing and implement information safeguards and regularly test /monitor their effectiveness.



What are the data security requirements? cont'd

- Oversee service providers, by:
 - 1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the FSA, student, & school (customer) information at issue
 - 2) Requiring your service providers by contract to implement and maintain such safeguards.
- Evaluate & adjust school's info-sec program in light of:
 - the results of the required testing /monitoring
 - any material changes to your operations or business arrangements;
 - any other circumstances that you know may have a material impact on your information security program.



What are the data security requirements? cont'd

- Title IV schools are subject to the requirements of the FTC **Identity Theft Red Flags Rule** (72 Fed. Reg. 63718) issued on November 9, 2007
- The “Red Flags Rule” requires an institution to develop and implement a written Identify Theft Prevention Program to:
 - Detect
 - Prevent
 - Respond to patterns, practices, or specific activities that may indicate *identity theft*



What is a breach?

- Per GLBA, a breach is *any unauthorized disclosure, misuse, alteration, destruction or other compromise of information.*
- Administrative, technical, and physical safeguards:
 - 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.



Important items to note:

- No minimum size or # of records
- Employee access is not exempt if wrong
- Not strictly digital or technology-based – **paper counts!**
- Covers data in storage, in transit or being processed

When do I report a breach?

- The Student Aid Internet Gateway (SAIG) Agreement requires that as a condition of continued participation in the federal student aid programs Title IV schools report suspected/actual data breaches
- Title IV schools must report **on the day of detection** when a data breach is even suspected
- The Department has the authority to fine institutions that do not comply with the requirement to self-report data breaches; up to **\$54,789 per violation** per 34 C.F.R. § 36.2
- The Department has reminded all institutions of this requirement through Dear Colleague Letters ([GEN 15-18](#), [GEN 16-12](#)), electronic announcements, and the annual FSA Handbook.



How do I report a data breach? (Yes, you!)

1. Email cpssaig@ed.gov & copy your data breach team, executives, per your policy

Data to include in the e-mail:

- Date of breach (suspected or known)
 - Impact of breach (# of records, etc.)
 - Method of breach (hack, accidental disclosure, etc.)
 - Information Security Program Point of Contact
 - Email and phone details will be necessary
 - Remediation Status (complete, in process – with detail)
 - Next steps (as needed)
2. Call Education Security Operations Center (ED SOC) at 202-245-6550 with above data. ED-SOC operates 7x24.
 3. Call or Email Tiina Rodrigue – tiina.rodrigue@ed.gov or 202-377-3887 – if both previous methods fail.



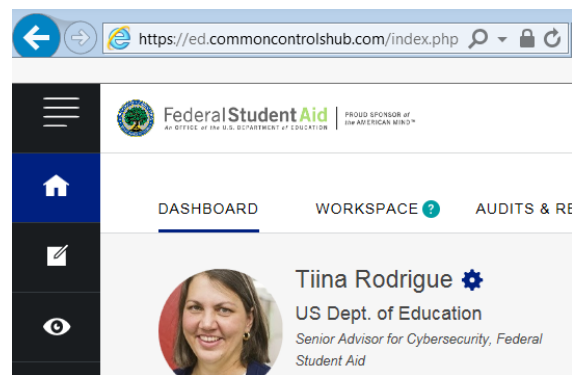
How can you help me with data security?



- [Cybersecurity Assessment Tool \(CAT\)](#) - optional self-assessment electronic tool that helps establish school's current risk profile and cybersecurity maturity for executive review & prioritization:
 - Built by [Federal Financial Institution Examiners' Council](#) (FFIEC) to help financial institutions review current state
 - Education has automated it to better enable schools of all levels to review current state of risk and maturity
 - Targets specific areas to address to close the gaps from a best practice perspective while preventing waste or over-engineering
 - Covers 5 Domains in depth, with diverse areas including culture, acquisitions, 3rd-party management which aligns with GLBA requirements
 - Pertains to policy, people and process issues, too

How can you help me with data security?

- [Institutions of Higher Education \(IHE\) Compliance Framework](https://ed.commoncontrolshub.com/index.php)
 - Public-Private Partnership to reduce the burden of compliance for security **and** privacy controls for Title IV schools
 - Register for a free account to access the optional tool & data
 - Driven by the regulation on a federal and state level
 - Includes the international regulations for foreign schools
 - Consolidates all relevant laws into one compliance framework
 - Prevents duplicate effort, saving the schools money and effort



Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION

PROUD SPONSOR of
the AMERICAN MIND™

How can you help me with data security?

NIST has provided non-FISMA guidelines ([800-171](#)) that are recommended by FSA & Education [in GEN 16-12](#) which gives specific technical standards to prove [GLBA](#) compliance:

- Access Control
- Awareness and Training
- Audit and Accountability
- Configuration Management
- Identification Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical Protection
- Risk Assessment Requirements
- Security Assessment Requirements
- System and Communications Protection
- System and Information Integrity

How can you help me with data security?

As an option, you can contact Senior Advisor – Cybersecurity to:

- Ask hypothetical questions – is this an area of concern?
- Get a consultative review – policy or process (it's free!)
- Use the tools or get additional information (also free)
- Collaborate on best practices or bring ideas forward
- Review new [Cybersecurity Compliance](#) page – send input

Contact information:

- Tiina Rodrigue – tiina.rodrigue@ed.gov
- 202-377-3887

What are my next steps?

1. Find your information security policy and program for your school - If you don't have one, develop one
2. Verify your school's information security policy and program has an individual with his/her contact information - Make sure to keep that person up to date in the policy and is actively managing the program
3. Verify that your school has information risk assessment/testing schedule in place - if you don't have one, develop one
4. Verify that your school has documented the tests and results based on that schedule - if haven't tested, have team start to follow the schedule and DOCUMENT it
5. Add your information security policy/program/schedule/contact information to your consumer information and compliance website so that you can easily find/maintain it
6. Communicate to your entire executive team so that if a breach happens, everyone is prepared to respond immediately & appropriately

Post-Secondary Institution Data-Security Overview and Requirements

Tiina K.O. Rodrigue, EdDc, CISSP, CISM, PMP, CSM,
CEA, ITIL, ISC2 Compliance Mapper, A+
Senior Advisor – Cybersecurity - 2017

The [GLBA Safeguards Rule](#) defines the following:

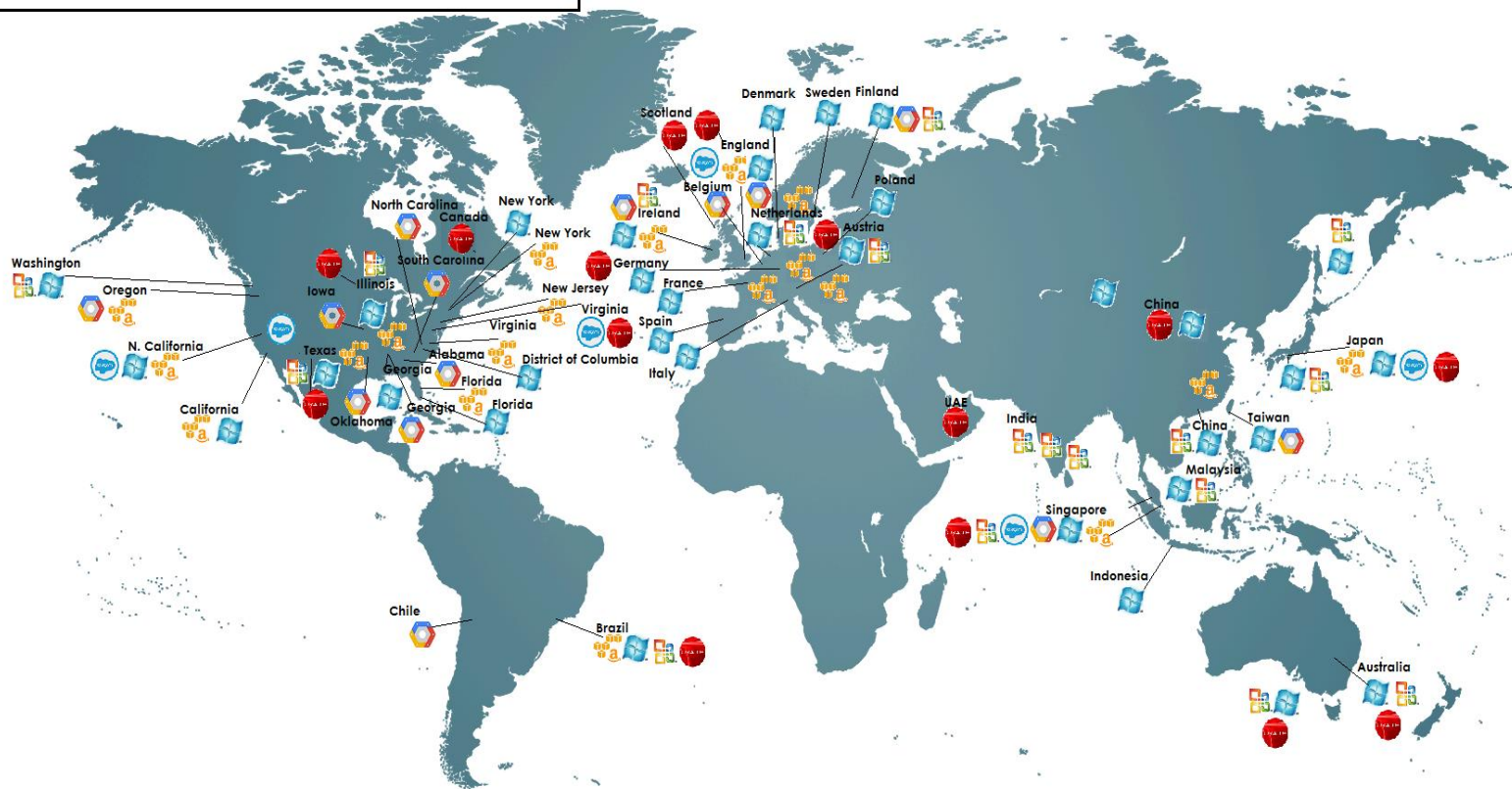
- An **information security program** is defined as the administrative, technical, or physical safeguards used to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.
- **Customer information** is defined as any record containing nonpublic personal information as defined in 16 CFR 313.3(n), about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of the financial institution or its affiliates.
- A **service provider** is defined as any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to the Safeguards Rule.

Federal Student Aid

An OFFICE of the U.S. DEPARTMENT of EDUCATION

PROUD SPONSOR of
the AMERICAN MIND™

Consolidated Cloud Global Footprint Map



Sources: MS O365 - <https://www.microsoft.com/online/legal/v2/?docid=25> | Amazon - <https://aws.amazon.com/about-aws/global-infrastructure/> | Google - <https://www.google.com/about/datacenters/inside/locations/index.html>
Salesforce - <https://help.salesforce.com/servlet/servlet.FileDownload?file=015300000035PzoAAE>, <http://www.cloudsuccess.com/blog/where-are-salesforce-com-data-centres/>, <http://www.datacenterknowledge.com/archives/2014/11/04/salesforce-com-data-center-opens-in-the-uk>
MS Azure - <http://www.iclouds.org/20141114/maps-of-data-center-localization/> | Map - http://play.ramjam.co.uk/travelsupermarket/img/TS_Map_Blue2.png | Oracle - <http://4.bp.blogspot.com/-pqFYOnLVJM8/VUQus8THB8I/AAAAAAAAIx8/IXNT4ocse>