

Compliance Potpourri!

Three Topics: State Authorization Reciprocity Agreement, Federal Cybersecurity Regulations, and Compliance Programs



The information provided here is of a general nature and is not intended to address the specific circumstances of any individual or entity. In specific circumstances, the services of a professional should be sought.

Webinar moderator



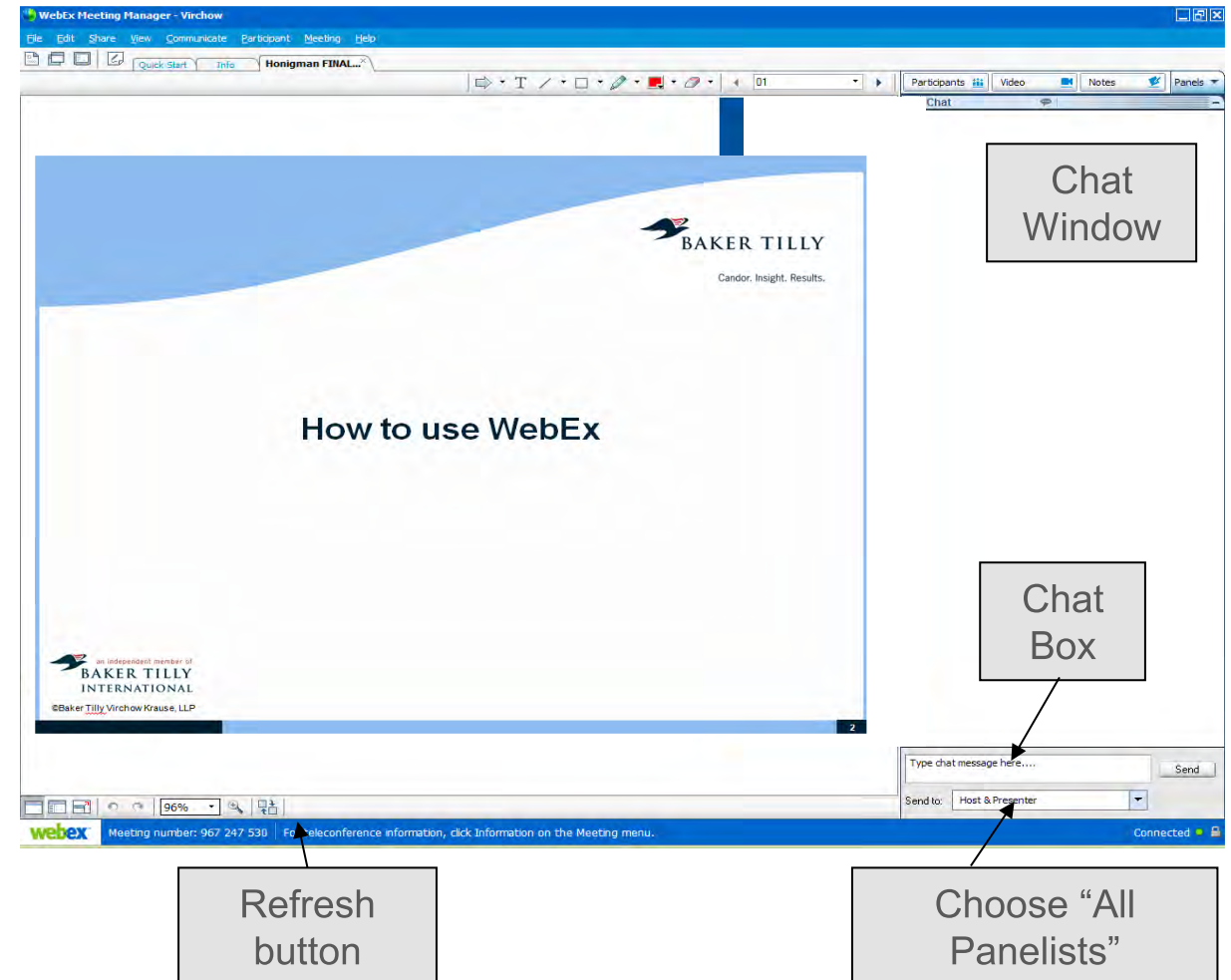
Jana Clark

ACUA Distance Learning Director
Senior Internal Auditor
Kansas State University



WebEx guide

- > **Everyone is muted** to avoid background noise. Please use the chat box if you need to communicate with the host
- > **Audio issues:** If you are unable to hear the speaker, call in to the webinar using the WebEx dial-in information
- > **Asking questions:** In the chat screen, ask questions by choosing “All Panelists” in lower right chat window. Type your message in the chat box and hit “send”
- > **If disconnected:** Refer to your e-mail and reconnect. If audio is disconnected, click the Communicate tab in the upper left to find the dial-in numbers and access code or refer back to your e-mail for the dial-in number
- > **Support:** If you have technical problems, call WebEx Support at 866 229 3239
- > **Recording:** We will be recording today



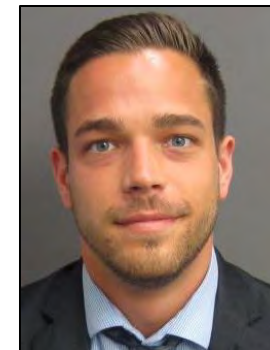
Your presenters



NATALY CHEREPANSKY
SENIOR CONSULTANT
Baker Tilly



JIMMY EDMUNDSON
SENIOR CONSULTANT
Baker Tilly



MATT YATES
CONSULTANT
Baker Tilly

Objectives



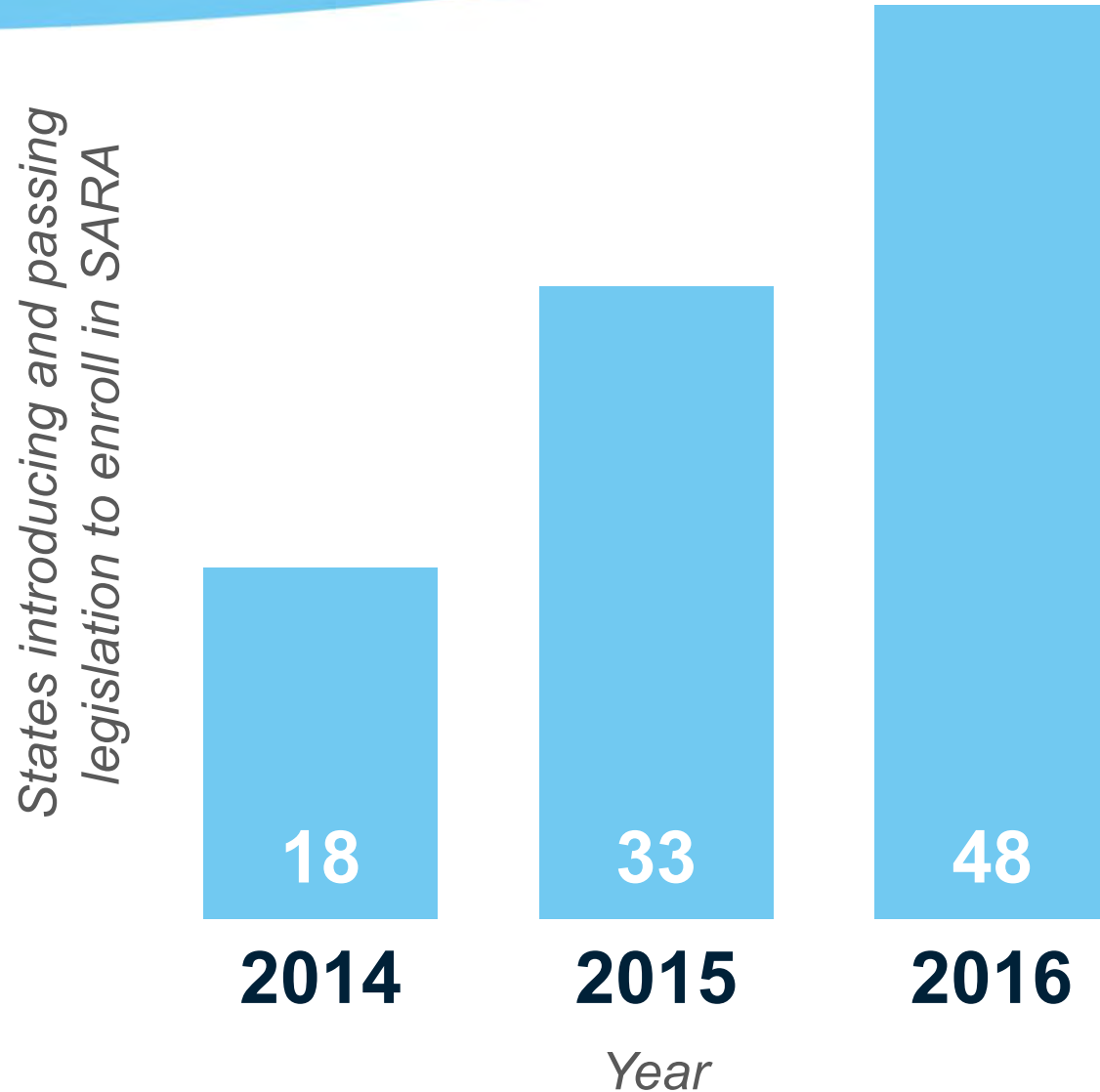
- > Understand how to leverage the State Authorization Reciprocity Agreement (SARA) framework to be in compliance with the Department of Education's (DOE) regulations regarding state authorization
- > Identify opportunities to enhance cybersecurity program safeguards related to compliance requirements under the Defense Federal Acquisition Regulation Supplement (DFARS) and the Gramm-Leach-Bliley Act (GLBA)
- > Leverage leading practices on collaboration initiatives for internal audit and compliance to effectively address key regulatory requirements

State Authorization Reciprocity Agreement



- > SARA simplifies authorization for colleges and universities to offer distance learning to students in other states. Similar to driver's licenses, SARA has to do with **reciprocity**
- > SARA helps institutions become compliant with **DOE regulations** without needing to individually register in each state in which its distance learning programs are offered
- > The **members of SARA are states, not institutions**. States “join” or becomes a “member” of SARA, while institutions “operate under” or “participate in” SARA

SARA member states



- > **47 states and Washington, DC** are currently members of SARA
- > The three states that are *not* members are **California, Florida, and Massachusetts**

Benefits of SARA



States

- > States **focus on their home state institutions**, rather than institutions from outside states
- > States continue to regulate on-the-ground instruction in their state that is offered by outside institutions
- > Other SARA states **help resolve complaints**

Institutions

- > There is **more efficient access** to distance education for a larger market
- > There are fewer out-of-state regulations to monitor and track
- > Applications and other state requirements are fewer
- > **Costs are reduced** for institutions, supporting affordability

SARA challenges – the Final Rule

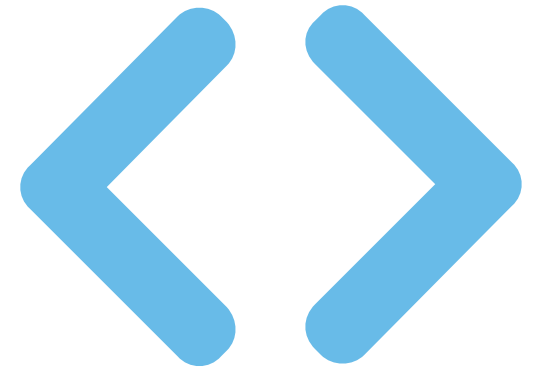


- > In December 2016, the DOE published the **Final Rule**, which amended the Department's 34 CFR § 600.9 regulations related to Title IV
- > The DOE **acknowledged SARA as a way to meet the Title IV program requirement**. If institutions do not have authorization in each state in which their distance learning program is offered, they must be able to document SARA approval
- > However, the Final Rule states **SARA cannot prevent a state's enforcement of its own laws**

SARA challenges



- > Institutions in the non-SARA member states (California, Florida, Massachusetts) **cannot participate** in SARA
- > States and institutions **must rely on other states** to regulate and monitor the operations of the other states' institutions



Potential auditing procedures



SARA Guideline	Guiding Questions
<ul style="list-style-type: none">> Online learning is appropriate to the institution's mission and purposes	<ul style="list-style-type: none">> Does your institution have an up-to-date mission statement?> Do the students admitted to the distance learning program meet applicable criteria, and do they align with the types of students the institution aims to serve?
<ul style="list-style-type: none">> The institution's plans for developing, sustaining, and, if appropriate, expanding online learning offerings are integrated into its regular planning and evaluation processes> Online learning is incorporated into the institution's systems of governance and academic oversight	<ul style="list-style-type: none">> Are there defined procedures and criteria for creating, and periodically assessing, the distance learning program's effectiveness?> Are the program's faculty members, rather than only members of administration, involved in creating and continuing to develop the program?

Potential auditing procedures



SARA Guideline	Guiding Questions
<ul style="list-style-type: none">> Curricula for the institution's online learning offerings are coherent, cohesive, and comparable in academic rigor to programs offered in traditional instructional formats	<ul style="list-style-type: none">> Are goals and objectives set at the beginning of each online course?> Do online courses follow a similar scheduling process and enable students to take classes timely to complete their degree?> Are the online course curricula similar to campus courses and lectures, and do they enable the achievement of the course's goals and objectives?
<ul style="list-style-type: none">> The institution evaluates the effectiveness of its online learning offerings, including the extent to which the online learning goals are achieved, and uses the results of its evaluations to enhance the attainment of the goals	<ul style="list-style-type: none">> Are there documented processes in place to assess whether the goals and objectives of the course are achieved?

Potential auditing procedures



SARA Guideline	Guiding Questions
<ul style="list-style-type: none">> Faculty responsible for delivering the online learning curricula and evaluating the students' success in achieving the online learning goals are appropriately qualified and effectively supported	<ul style="list-style-type: none">> Do online faculty and instructors follow the same training procedures as in-person faculty and instructors?> Are the persons or offices responsible for online learning training programs clearly identified and qualified to accomplish the tasks?
<ul style="list-style-type: none">> The institution provides effective student and academic services to support students enrolled in online learning offerings	<ul style="list-style-type: none">> Do online students have the same student support services as in-person students (e.g., online orientation, financial aid, course registration, learning resources such as libraries and online databases)?> Are there student surveys to assess whether online students have sufficient technical and educational support? What is the process for following up on survey results?

Potential auditing procedures



SARA Guideline	Guiding Questions
<ul style="list-style-type: none">> The institution provides sufficient resources to support and, if appropriate, expand its online learning offerings	<ul style="list-style-type: none">> Is distance learning documented as a key component of the institution's mission and goals?
<ul style="list-style-type: none">> The institution assures the integrity of its online offerings	<ul style="list-style-type: none">> Do the institution's policies and procedures explicitly refer to online learning?> Are there policies and procedures in place to confirm the identities of students enrolled in online courses, and confirm that the students enrolled are the individuals participating in the course?

SARA resources



- > NC-SARA website: <http://www.nc-sara.org/>
- > State actions regarding SARA: <http://www.nc-sara.org/state-actions/state-actions-regarding-sara>
- > SARA policy and operations manual: http://www.nc-sara.org/files/docs/NC-SARA_Manual_Final_2016.pdf
- > SARA institutional application: http://www.nc-sara.org/files/docs/SARA-Institutional-Application_122116_final.pdf

Federal cybersecurity regulations



Gramm-Leach-Bliley Act

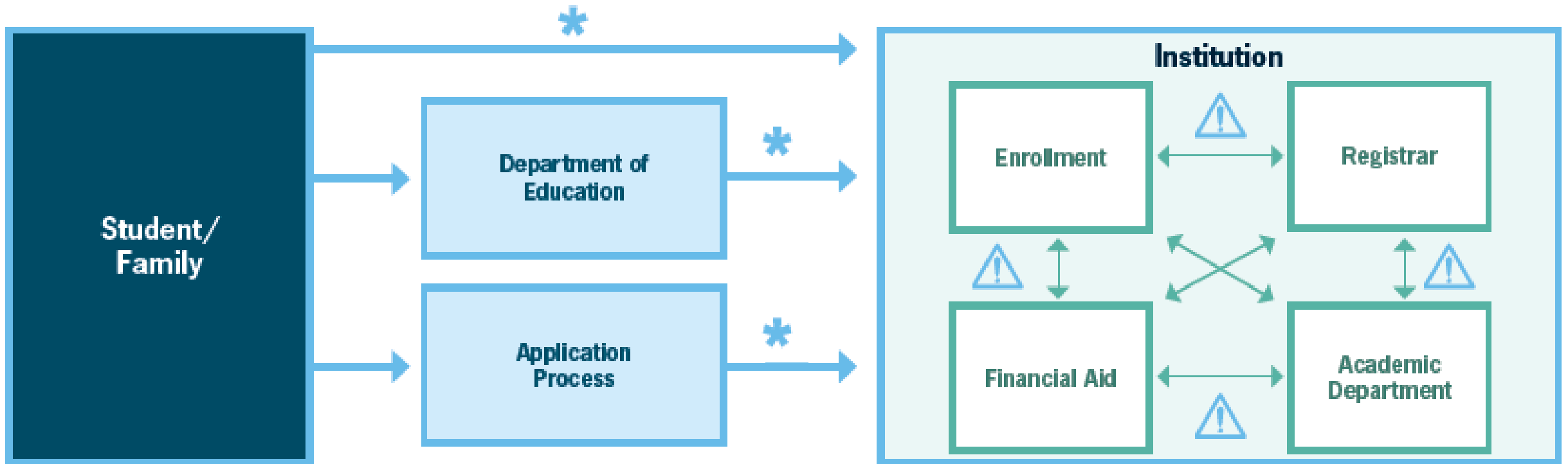
Overview of Gramm-Leach-Bliley Act:

- > Two major components: Safeguards Rule and Privacy Rule
- > Safeguards Rule: An institution must **establish safeguards to ensure proper security of personal information**, including:
 - Designate a security program coordinator responsible for coordinating the program
 - Conduct a risk assessment to identify reasonably foreseeable security and privacy risks
 - Establish a written information security plan that describes how safeguards are employed to control the identified risks; regularly test and monitor the effectiveness of these safeguards
- > Privacy Rule: Requires institutions to **explain their information-sharing practices** to their customers (e.g., students)
 - Privacy Notice must include how you protect confidentiality of students' data

Dear Colleague Letter (DCL) on cybersecurity requirements for financial aid data:


- > ED's 2016 DCL reiterates the legal obligations of institutions to **protect confidential student information** used in the administration of Title IV financial aid programs
- > Six GLBA requirements referenced in the DCL:
 - Develop, implement, and maintain a written information security program
 - Designate the personnel responsible for coordinating the information security program
 - Identify and assess risks to consumer nonpublic personal information
 - Design and implement an information safeguards program
 - Select appropriate service providers that are capable of maintaining appropriate safeguards
 - Periodically evaluate and update the information security program

Common risks in typical financial aid data flows



 **Risks**

- > Transmission methods vary
- > Paper and electronic files
- > Data is outside the institution's control

 **Risks**

- > Staff access to data/system
- > Transmission methods vary
- > Data retention/storage

Example audit objectives / tips:

- > Ensure an institution's **Gramm-Leach-Bliley policy** exists and that it includes an information security plan
- > Meet with select departments to assess their awareness of, and compliance to, the **safeguard rules of information security**
- > Evaluate compliance practices related to **information sharing**
- > Review **background/reference checks** on personnel
- > Validate **regular trainings** on the institution's policy and legal requirements occur
- > Analyze **system access** and practices
- > Review files and programs that reveal how **data breaches** have occurred

What other institutions are doing:

- > Getting their information security policies in order (written and finalized)
 - Ensuring the policies contain administrative, technical, and physical safeguards that are appropriate to the size and complexity of the entity and the nature and scope of its activities
- > Continually **identifying potential risks**
- > Keeping standards current
- > Securing both nonpublic and public personal information
- > **Notifying students of the privacy policy** on an annual basis (don't just bury it somewhere on the Web site)
- > **Encrypting data** both in storage and in transit

GLBA resources



- > Dear Colleague Letter 2016: <https://ifap.ed.gov/dpcletters/GEN1612.html>
- > Dear Colleague Letter 2015: <https://ifap.ed.gov/dpcletters/GEN1518.html>
- > Gramm-Leach Bliley Act: <https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act>
- > NACUBO GLBA:
http://www.nacubo.org/Business_and_Policy_Areas/Privacy_and_Intellectual_Property/GLBA_Resources.html
- > EDUCAUSE GLBA:
 - > <http://er.educause.edu/blogs/2017/4/glba-safeguards-rule-auditing-delayed-to-fy18-audits>
 - > <https://library.educause.edu/~media/files/library/2016/11/ftcsafeguardsrulerfcresponse.pdf>
 - > <http://er.educause.edu/blogs/2017/4/update-pending-fsa-audit-requirement-on-safeguards-rule>

Cyber DFARS



What is federal information?

CDI

Covered Defense Information – Unclassified information provided to the contractor by or on behalf of DoD in connection with the performance of the contract, or collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract (see DFARS 252.204-7012)

Controlled Unclassified Information – Information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls, excluding information that is classified (see Executive Order 13556 and CUI Registry at www.archives.gov/cui)

CUI

FCI

Federal Contract Information – *Any* information provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, *but not including* information provided to the public (e.g., publicly accessible website data) or simple transactional data (e.g., billing or payment processing data)

DFARS 252.204-7012
“Safeguarding Covered
Defense Information
and Cyber Incident
Reporting”

> Provides guidance to Federal Defense and Aerospace contractors around CDI and reporting cyber incidents affecting contractor information systems – or CDI residing within those systems – to the Federal Government, and requires contractors to do the following:

- Implement **adequate cybersecurity safeguarding controls** on all covered contractor information systems in accordance with specific frameworks and standards set forth in the ruling
- **Rapidly report cyber incidents** affecting contractor information systems or CDI residing within those systems to the Federal Government

IMPLEMENTATION OF ADEQUATE CYBERSECURITY SAFEGUARDING CONTROLS:

DFARS 252.204-7012
“Safeguarding Covered
Defense Information
and Cyber Incident
Reporting”

continued

- > Where contractor is handling CDI on their systems, must implement safeguarding controls according to **NIST SP 800-171**
- > For systems operated on behalf of the government, see specific contract guidance and/or **DFARS 252.239-7010 “Cloud Computing Services”** if applicable
- > Any other such services or systems (e.g., other than cloud computing) are subject to the security requirements specified in those contracts
- > All contractors, subcontractors, suppliers, and partners must implement NIST SP 800-171 security requirements by December 31, 2017

REPORTING OF CYBER INCIDENTS

DFARS 252.204-7012
“Safeguarding Covered
Defense Information
and Cyber Incident
Reporting”

continued

- > A **cyber incident** is any action taken through computer networks resulting in the compromise, or an actual or potentially adverse effect, of an information system and/or the information residing within those systems
- > Cyber incidents shall **be reported to DoD within 72 hours** of discovery via DoD’s Defense Industrial Base (DIB) Cyber Incident Reporting & Cyber Threat Information Sharing Portal
- > Contractors must acquire a DoD-approved medium assurance certificate from Defense Information Systems Agency (DISA) to access the DIB portal
- > Subcontractors who handle CDI under prime contracts with the Federal Government are required to report cyber incidents directly to DoD and their prime contractor customers (or next higher-tier subcontractor)

NIST SP 800-171
“Protecting Controlled
Unclassified
Information in
Nonfederal
Information Systems
and Organizations”
Revision 1

- > Agencies must use NIST SP 800-171 when establishing security requirements to protect CUI’s confidentiality on *non-Federal information systems* (e.g. contractors’ systems)
- > Intended for use by federal agencies in appropriate contractual vehicles or other agreements established between those agencies and nonfederal organizations (e.g. contractors)
- > NIST SP 800-171 should be used when a contractor receives CDI/CUI incidental to providing a service or product to the Government (e.g., producing a study, conducting research, creating training, etc.)
- > Describes 110 total controls across 14 control families
- > Provides mapping to **NIST SP 800-53 Revision 4** and **ISO 27001** information security controls

Who is impacted?



All contractors who handle CDI are impacted by the Cyber DFAR

... For subcontractors and suppliers, flow-down requirements apply

- > Subcontractors are ultimately responsible for implementing cybersecurity safeguarding controls to be in compliance
- > Subcontractors will be held accountable for breaches if they have not implemented required controls
- > Prime contractors may be impacted by breaches involving their subcontractors
 - Prime contractors may proactively engage key subcontractors to understand their current security posture and assess risk to their contracts
 - Collaborative solutions are being implemented to capture information on subcontractors' cybersecurity safeguarding practices

How can you become compliant?



1

Identify and inventory all contracts and CDI

- > Focus on contracts where CDI may be potentially involved
- > Identify “high risk” contracts, including current bid and proposal efforts (e.g., potential new awards)
- > Consider prime-sub relationships
- > Identify system boundaries for handling

2

Understand cybersecurity requirements

- > Focus on language around protection of information and reporting requirements
- > Identify specific guidance references
- > Do not be afraid to engage your CO and / or CISO

3

Assess current state of cybersecurity controls

- > Use appropriate security control guidance (NIST SP 800-171)
- > Where is your federal information stored, processed, and / or transmitted?
- > What controls do you have in place?
- > Conduct gap analysis and determine necessary corrective actions

4

Develop cybersecurity action plan

- > Develop detailed list of prioritized corrective actions with assigned owners and target completion dates
- > Define roles and responsibilities with oversight
- > Redefine system boundaries for handling CDI as necessary

5

Execute cybersecurity action plan

- > Respond to agency and / or prime contract officers with results of your assessment
- > Implement security controls
- > Establish monitoring and reporting practices

6

Monitor cybersecurity compliance practices

- > Monitor progress of ongoing implementation efforts
- > Regularly evaluate effectiveness of cybersecurity controls via ongoing testing and third-party assessments
- > Monitor regulatory environment for new developments (e.g., laws, standards, and policies)

What other institutions are doing



Engage third parties for assistance with compliance efforts

Minimize exposure to covered contractor information systems

Conduct a gap assessment to identify compliance gaps

Regularly assess and monitor progress towards remediation of known gaps

Monitor regulatory landscape for changes and new developments

- > DFARS 252.204-7012:
<http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012>
- > CUI Registry: www.archives.gov/cui
- > NIST SP 800-171 for Higher Ed:
<https://library.educause.edu/resources/2016/4/an-introduction-to-nist-special-publication-800-171-for-higher-education-institutions>

Internal audit and compliance collaboration



Overview



- > Understand the importance of an integrated approach between internal audit (IA) and compliance
- > Discuss how collaboration results in a more effective compliance program
- > Provide examples and leading practices for institutional collaboration between IA and compliance and functions
- > Review a case study example of our success with IA and compliance collaboration



Challenges faced by independent IA and compliance functions

- > Increasing legal / regulatory demands and subsequent risk of non-compliance
- > Technical / skilled resources to support changing institutional needs (e.g. information technology [IT])
- > Limited institutional budgets and resources
- > Overly-complex institutional environment
- > Confidentiality of information (e.g., conflicts of interest disclosures, privacy issues)

Benefits of collaboration

IA and compliance collaboration provides opportunities for:

- > Improved performance
- > Streamlined processes
- > More efficient use of limited institutional resources
- > Simplified communication channels
- > More informed decision making



Tools

- > Information sharing platforms (e.g., Huddle, SharePoint, other cloud-based options)
- > Activity trackers
 - Audits
 - Reported items and work log follow-up
 - Policy updates / reviews
- > University communication networks (e.g., compliance hotline)
 - Software tool for automated tracking, monitoring, following-up and reporting
- > Inventory of compliance-based regulatory risks
 - Risk assessments



Techniques

- > Collaboration with overlapping initiatives (e.g., meeting regularly)
- > Inform IA of potential concerns to help plan potential future audit areas
- > Review audit results and discuss observations to inform activities
- > Communicate operational challenges that are reported through compliance resources (e.g., compliance reporting hotline, stakeholder meetings)
- > Schedule meetings with various stakeholders and members of university leadership to share compliance focus areas and offer support

Client

- > Baker Tilly serves as the compliance function at a complex, private research institution
- > IA reviewed the institution's procurement to payment (P2P) process, which required subsequent updates to the outdated P2P policy (compliance owns policy review / update process)

Solution

- > Compliance and IA facilitated regular meetings to ensure buy-in / approval from upper-level leadership and process owners
- > IA informed compliance of the P2P audit findings and recommendations
- > Compliance worked with the P2P Policy Owner to review and update the P2P policy

Results

- > Changes to the institution's P2P processes and updates to the P2P policy and related information were simultaneously implemented and communicated to faculty and staff members

Internal audit and compliance resources



- > The Society of Corporate Compliance and Ethics (SCCE): <http://www.corporatecompliance.org/>
- > The Institute of Internal Auditors: <https://na.theiia.org>
- > Regulatory compliance: <http://www.bakertilly.com/services/risk-internal-audit-cybersecurity/regulatory-compliance/>
- > Baker Tilly compliance handout

Contact information



Thank you for participating today! Remember CPE certificates will be emailed to you by ACUA Headquarters in approximately three weeks.

Nataly Cherepansky, CIA

> nataly.cherepansky@bakertilly.com

> 703 923 8466

Matt Yates

> matt.yates@bakertilly.com

> 703 923 8532

Jimmy Edmundson, CISA, HITRUST CCSFP

> jimmy.edmundson@bakertilly.com

> 703 923 8293



Upcoming events

- > **August 16, 2017** – Business Continuity: What’s at Risk with Mark Bednarz & Larry Baye from PKF O’Connor Davies
- > **August 22, 2017** – HIPAA with Baker Tilly
- > **September 13, 2017** – Data Privacy with Mark Bednarz and Michael Cox from PKF O’Connor Davies
- > **September 24-28, 2017** – ACUA Annual Conference in Phoenix, AZ
- > **October 12, 2017** – Grant Fraud Detection with Melissa Hall from Georgia Tech and Paul Coleman, consultant

