UNIVERSITY SYSTEM OF GEORGIA

REGULATORY REQUIREMENTS SUPPORTING CYBERSECURITY AWARENESS TRAINING: A USG IT HANDBOOK COMPANION GUIDE

VERSION 2

2/20/2021

PUBLIC

Abstract: This companion guide was developed to aid USG organizations concerning the regulatory requirements surrounding cybersecurity awareness training and has been classified as a "Public" document.

Revision & Sign-off

Change Record

Date	Author	Version	Change Reference
20210220	Alfred Barker	1	Initial review
20210223	Alfred Barker	2	Add P.L. 100-235

Document Properties

Item	Details
Document Title	Regulatory Requirements Supporting Cybersecurity Awareness Training: A USG IT Handbook Companion Guide
Document Type	Guideline (Internal Use Only)
Author	Alfred Barker
Document Manager	Alfred Barker
Creation Date	20201009
Last Updated	20210223
Document Classification	Public

Introduction

This guideline is classified as Public and was developed for internal use. The purpose of the guideline is to complement the *USG IT Handbook* by providing regulatory requirements concerning cybersecurity awareness and training.

The examples provided may or may not apply to your organization and need to be assessed for applicability. For example, New York State's requirements may have no bearing on your organization unless your organization is doing business in or with New York. Whereas, other regulations like GLBA will affect all USG organizations. These requirements were added because of past precedent. Like breach notification, it took only one state to pass into law breach requirements for notification, and currently all states have breach notification legislation. The same trend is happening at the state level concerning data privacy. Raising awareness as to what one state has formalized into law, we may predict what the future of awareness training legislation may look like in the near future.

Board Policy *10.4.2 Institutional and Organizational Level Responsibilities* states, "Cybersecurity implementation must include a user awareness, training, and education plan, which is consistent with the guidelines provided by USG Cybersecurity and shall be submitted to USG Cybersecurity for review upon request. Methods for ensuring that applicable laws, regulations, guidelines, and policies concerning cybersecurity awareness training are followed shall be distributed and readily available to each organization's user community."

It is the section underlined above that this document intends to address. USG Cybersecurity has researched many common regulations to provide the following international, federal, state, local, and industry listing of awareness training requirements.

International Law

General Data Protection Regulation (GDPR)

Under Article 39, the GDPR includes among the tasks of the Data Protection Officer (DPO) "awareness raising, and training of staff involved in the processing operations." Under Article 47, in connection with Binding Corporate Rules (BCRs), the GDPR requires "the appropriate data protection training to personnel having permanent or regular access to personal data."

GDPR Article 39. The Tasks of the Data Protection Officer

> 1. The data protection officer shall have at least the following tasks:
>
> (b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising, and training of staff involved in processing operations, and the related audits; ….

GDPR Article 47(2). Binding Corporate Rules

> 2. The binding corporate rules referred to in paragraph 1 shall specify at least ….
>
> (n) the appropriate data protection training to personnel having permanent or regular access to personal data.

Personal Information Protection and Electronic Document Act (PIPEDA)

Principle 4.1.4 of PIPEDA, Canada's broadly applicable privacy law, requires training about the "organization's policies and practices" related to complying with PIPEDA.

PIPEDA Principle 4.1.4

> Organizations shall implement policies and practices to give effect to the principles, including ...
>
> (c) Training staff and communicating to staff information about the organization's policies and practices.

US Federal Laws, Regulations, and Treaties

Computer Security Act

The Computer Security Act of 1987 (Public Law (P.L.) 100-235) is to provide a standard, "for government-wide computer security, and to provide for the training in security maters of persons who are involved in the management, operation and use of… computer systems."

- P.L. 100-235 § 5(a) In General – "Each… shall provide for the mandatory periodic training in computer security awareness…."
- P.L. 100-235 § 5(b) Training Objectives – To raise awareness of the threats and vulnerabilities of computer systems…" and, "encourage the use of improved computer security practices."

Federal Education Rights and Privacy Act (FERPA)

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education 12.5 Compliance.

34 CFR Part 99.62 What information must an educational agency or institution or other recipient of Department funds submit to the Office?

> "The Office may require an educational agency or institution… to submit reports, information on policies and procedures, annual notifications, training materials, or other information necessary to carry out the Office's enforcement responsibilities under the Act or this part."

The following is USGs Business Procedures Manual's requirements concerning FERPA compliance.

- BPM 12.5.1 Regulatory Compliance

  Closely managing data content is necessary to ensure compliance with federal, state and local regulations as well as grants and contract specifications. Each USG organization is responsible for clearly understanding and managing data to ensure confidential data is appropriately classified and safeguarded. Each USG organization must have policies and procedures to ensure that appropriate organizational personnel has a working knowledge of:

  - Family Education Rights and Privacy Act (FERPA) ….

- BPM 12.5.2 Training

The purpose of this section is to ensure that appropriate individuals at each USG organization receive training on the data governance policies, procedures, and roles developed in compliance with preceding requirements in this Data Governance and Management section.

Organizations must:

- Provide role specific training to all individuals within the data governance structure, including data users and all those subject to data governance policies; …
- Provide training to individuals as they enter these roles, when there are substantive changes to training and at regular intervals over time to ensure up-to-date understanding;
- Update training materials as changes to policy and procedure require;
- Document participation in training and audit training participation at regular intervals;
- Provide training materials in a permanent form (such as on a website) for individuals to reference as needed; [and,]
- Specifically address in training materials for all individuals how data classified as public or protected is managed throughout its lifecycle ….

Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules

HIPAA's Privacy and Security Rules have extensive training requirements. HIPAA requires a covered entity to train all workforce members on its policies and procedures with respect to personal health information PHI. Each new workforce member must be trained within a reasonable period after hiring. Thereafter, training must be given whenever there is a material change in policies or procedures. Covered entities and business associates must provide a security awareness and training program for all workforce members. This program must include periodic security updates.

45 CFR § 164.530 Administrative requirements.

(b)(1) *Standard: Training.* A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart and subpart D of this part, as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity.

(2) *Implementation specifications: Training.*

(i) A covered entity must provide training that meets the requirements of paragraph (b)(1) of this section, as follows:

(A) To each member of the covered entity's workforce by no later than the compliance date for the covered entity;

(B) Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and

(C) To each member of the covered entity's workforce whose functions are affected by a material change in the policies or procedures required by this subpart or subpart D of this part, within a reasonable period after the material change becomes effective in accordance with paragraph (i) of this section.

(ii) A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been provided….

45 CFR § 164.308(a)(5) Administrative safeguards.

(a)(5)(i) Standard: Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management).

Gramm-Leach-Bliley Act (GLBA)

Training under GLBA is required via the Safeguards Rule, 16 CFR 314.4. The training requirement is rather vague, but interagency guidance recommends that organizations should: "Train staff to recognize and respond to schemes to commit fraud or identity theft, such as guarding against pretext calling; provide staff members responsible for building or maintaining computer systems and local and wide-area networks with adequate training, including instruction about computer security; and train staff to properly dispose of customer information."

GLBA Safeguards Rule, 16 CFR 314.4

(b) Identify reasonably foreseeable internal and external risks . . . including (1) Employee training and management.

FACTA – Federal Trade Commission (FTC) Red Flags Rule

Under the Fair and Accurate Credit Transaction Act (FACTA), the FTC established the Red Flags Rule, which requires training as part of an Identity Theft Prevention Program (16 CFR 681.1(d)-(e)). Staff should receive training concerning various red flags impacting data security and privacy, and any other relevant aspect of the organization's Identity Theft Prevention Program.

16 CFR 681.1 - Duties regarding the detection, prevention, and mitigation of identity theft

(d) Establishment of an Identity Theft Prevention Program

(e) Administration of the Program. Each financial institution or creditor that is required to implement a Program must provide for the continued administration of the Program and must: …

(3) Train staff, as necessary, to effectively implement the Program ....

Federal Information Security Management Act (FISMA)

Federal agencies are required to establish a security awareness training program as defined in FISMA, 4 U.S.C. § 3544. The program must include contractors and "other uses of information systems" that support the agency. The program must address information security risks and each employee's responsibilities in complying with agency policies and procedures to minimize security risks.

(b) Agency program. – Each agency shall develop, document, and implement an agency wide information security program... that includes

(4) Security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency….

Federal Acquisitions Regulation (FAR)

As provided in the Federal Register, 81 FR 93476 (Dec. 20, 2016) (effective Jan. 19, 2017), federal contractors are required to have "initial training" for their workforce on privacy as well as "annual training thereafter." The training should cover the provisions of the Federal Privacy Act, penalties for violating the act, appropriate handling and safeguarding of personally identifiable information (PII), authorized uses of PII and procedures to be followed in the event of a data breach resulting in exposure.

24.301 Privacy training

(a) Contractors are responsible for ensuring that initial privacy training, and annual privacy training thereafter, is completed by contractor employees who

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information on behalf of the agency; or

(3) Design, develop, maintain, or operate a system of records (see FAR subpart 24.1 and 39.105).

(b) Privacy training shall address the key elements necessary for ensuring the safeguarding of personally identifiable information or a system of records. The training shall be role-based, provide foundational as well as more advanced levels of training, and have measures in place to test the knowledge level of users. At a minimum, the privacy training shall cover

(1) The provisions of the Privacy Act of 1974 (5 U.S.C. 552a), including penalties for violations of the Act;

(2) The appropriate handling and safeguarding of personally identifiable information;

(3) The authorized and official use of a system of records or any other personally identifiable information;

(4) The restriction on the use of unauthorized equipment to create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise access personally identifiable information;

(5) The prohibition against the unauthorized use of a system of records or unauthorized disclosure, access, handling, or use of personally identifiable information; and

(6) Procedures to be followed in the event of a suspected or confirmed breach of a system of records or unauthorized disclosure, access, handling, or use of personally identifiable information.

(c) The contractor may provide its own training or use the training of another agency unless the contracting agency specifies that only its agency-provided training is acceptable (see 24.302(b)).

(d) The contractor is required to maintain and, upon request, to provide documentation of completion of privacy training for all applicable employees.

(e) No contractor employee shall be permitted to have or retain access to a system of records, create, collect, use, process, store, maintain, disseminate, disclose, or dispose, or otherwise handle personally identifiable information, or design, develop, maintain, or operate a system of records, unless the employee has completed privacy training that, at a minimum, addresses the elements in paragraph (b) of this section.

EU-US Privacy Shield Framework

Proper training is necessary for an organization to comply with the Department of Commerce's Privacy Shield Framework. In its 7th Supplemental Principle (a series of principles that follows the primary 7 principles), called "Verification," Privacy Shield requires verification via self-assessment. One area to be attested is the organization must have "a published privacy policy regarding personal information" that "conforms to the Privacy Shield Principles" and that it "has in place procedures for training employees in its implementation." There is little guidance concerning the specifics of such training, but it should logically focus on ensuring compliance with the Privacy Shield principles.

7. Verification

c. Under the self-assessment approach, such verification must indicate that an organization's published privacy policy regarding personal information received from the EU is accurate, comprehensive, prominently displayed, completely implemented, and accessible. It must also indicate that its privacy policy conforms to the Privacy Shield Principles; that individuals are informed of any in-house arrangements for handling complaints and of the independent mechanisms through which they may pursue complaints; that it has in place procedures for training employees in its implementation, and disciplining them for failure to follow it; and that it has in place internal procedures for periodically conducting objective reviews of compliance with the above.

US State Laws, Regulations and Directives

The following are examples of state legislation governing cyber awareness training requirements. It is important to note these are provided in the event your organization conducts business with or in these states.

Georgia, Governor's Executive Order

The Governor's Executive Order dated August 13, 2019, ordered "mandatory semiannual cybersecurity training" for all "executive branch agencies." Additionally, cybersecurity training is ordered to take place within 90 days of the signing of the Executive Order.

<u>Ordered: Mandatory Cybersecurity Training</u>

Semiannual training for all Executive Branch agencies. All Executive Branch agencies shall ensure that employees complete at least one form of cybersecurity training within ninety (90) days of this Executive Order. An employee's failure to comply with this Order shall result in formal disciplinary action ….

Georgia Cybersecurity Board

The Cybersecurity Board, reconstituted by Executive Order on August 13, 2019, is tasked with identifying risks, promoting best practices, and assessing compliance with training.

Memo Dated January 29, 2020: Recommendations from the Georgia Cybersecurity Board

4. The Office of Information Security [GTA] provided additional guidance… for ongoing cyber training compliance, campaign, and reporting. Executive agencies are highly encouraged to utilize… training software as their primary training platform.

   Rationale: [Training software] will create a streamlined reporting process… and minimize expenditure of state funds on duplicative efforts.

Massachusetts Data Security Law

Massachusetts's Data Security Law, at 201 CMR 17.03, requires training as mandatory for maintaining a comprehensive information security program. Training should focus on reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper, or other records containing personal information. Training must be "ongoing" and must be given for not only permanent employees but also temporary and contract employees.

201 CMR 17.03: Duty to Protect and Standards for Protecting Personal Information

(2) Without limiting the generality of the foregoing, every comprehensive information security program shall include, but shall not be limited to: …

(b) Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to: 1. ongoing employee (including temporary and contract employee) training ....

17.04: Computer System Security Requirements

(8) Education and training of employees on the proper use of the computer security system and the importance of personal information security.

New York Cybersecurity Regulation

New York's Cybersecurity Regulation, 23 NYCRR 500, has two sections that addresses training of organizational personnel. The first section addresses cybersecurity personnel specifically and the second section then applies to all personnel.

Section 500.10 Cybersecurity Personnel and Intelligence

(a) Cybersecurity Personnel and Intelligence. In addition to the requirements set forth in section 500.04(a) of this Part, each Covered Entity shall: …

(2) provide cybersecurity personnel with cybersecurity updates and training sufficient to address relevant cybersecurity risks; and

(3) verify that key cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures.

Section 500.14 Training and Monitoring

As part of its cybersecurity program, each Covered Entity shall: …

> (b) provide regular cybersecurity awareness training for all personnel that is updated to reflect risks identified by the Covered Entity in its Risk Assessment.

Texas Health Privacy Law

Section 181.101 of the Health and Safety Code, as amended by HB 1609, requires training that covers both the state's law and HIPAA. This law is one of the few state health laws that mandates training about the state's own health privacy law. Penalties and sanctions for violating the Texas law are equivalent to HIPAA's.

Section 181.101. Training Required

> (a) Each covered entity shall provide training to employees of the covered entity regarding the state and federal law concerning protected health information as necessary and appropriate for the employees to carry out their duties for the covered entity.
>
> (b) An employee of a covered entity must complete training described by Subsection (a) not later than the 180th day after the date the employee is hired by the covered entity.
>
> (c) If the duties of an employee of a covered entity are affected by a material change in state or federal law concerning protected health information, the employee shall receive training described by Subsection (a) within a reasonable period, not to exceed one year, after the material change becomes effective.
>
> (d) A covered entity shall require an employee of the entity who is trained as described by Subsection (a) to sign, electronically or in writing, a statement verifying the employee's completion of training. The covered entity shall maintain the signed statement for six years.

Standards and Policy

Payment Card Industry Data Security Standard (PCI-DSS)

PCI-DSS is a standard developed by the credit card industry's PCI council. It has a number of requirements regarding privacy training.

- PCI-DSS 12.6 – Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.
- PCI-DSS 12.6.1 – Educate personnel upon hire and at least annually.
- PCI-DSS 12.6.1.a – Verify that the security awareness program provides multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web-based training, meetings, and promotions).
- PCI-DSS 12.6.1.b – Verify that personnel attend awareness training upon hire and at least annually.
- PCI-DSS 12.6.2 – Verify that the security awareness program requires personnel to acknowledge, in writing or electronically, at least annually that they have read and understand the information security policy.

- PCI-DSS 12.9.4 – Verify through observation and review of policies that staff with responsibilities for security breach response are periodically trained.

ISO/IEC 27002

The International Standards Organization (ISO)'s Information Security standard ISO/IEC 27002:2005 is one of the most frequently followed standards by organizations throughout the world. The standard provides guidance on information security management in organizations, and it contains a requirement that all employees receive data security awareness training.

Section 8.2.2 Information Security Awareness, Education, and Training

> All employees of the organization and, where relevant, contractors and third-party users, should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.

NIST Special Publication 800-53 (Revision 4)

NIST SP 800-53 is one of the most relied-upon cybersecurity standards. Many federal agencies and state and local governments look to NIST to guide their rulemaking and enforcement. NIST SP 800-53 has extensive cybersecurity awareness training requirements as well as privacy awareness training requirements.

AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

Control: The organization:

> a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
>
> > 1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
> >
> > 2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and
>
> b. Reviews and updates the current:
>
> > 1. Security awareness and training policy [Assignment: organization-defined frequency]; and

2. Security awareness and training procedures [Assignment: organization-defined frequency].

AT-2 SECURITY AWARENESS TRAINING

Control: 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 ….

AT-3 ROLE-BASED SECURITY TRAINING

Control: The organization provides role-based security training to personnel with assigned security roles and responsibilities:

a. Before authorizing access to the information system or performing assigned duties;
b. When required by information system changes; and
c. [*Assignment: organization-defined frequency*] thereafter.

AT-4 SECURITY TRAINING RECORDS

Control: The organization:

a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and

b. Retains individual training records for [*Assignment: organization-defined time period*].

AR-5 PRIVACY AWARENESS AND TRAINING

Control: The organization:

a. Develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures;

b. Administers basic privacy training [*Assignment: organization-defined frequency, at least annually*] and targeted, role-based privacy training for personnel having responsibility for personally identifiable information (PII) or for activities that involve PII [*Assignment: organization-defined frequency, at least annually*] ….

USG Board of Regents Policy Manual

Section 10.4.2 of the USG Board of Regents Policy Manual addresses Institutional Responsibilities concerning user awareness training and is part of a larger USG cybersecurity policy.

Cybersecurity implementation must include a user awareness, training, and education plan, which is consistent with the guidelines provided by USG Cybersecurity and shall be submitted to USG Cybersecurity for review upon request. Methods for ensuring that applicable laws, regulations, guidelines, and policies concerning cybersecurity awareness training are followed shall be distributed and readily available to each organization's user community.

Chancellor's Memorandum concerning "Cybersecurity Awareness Month"

On October 2, 2019, the Chancellor issued a memorandum to "University System of Georgia Employees" to clarify and emphasize the importance of cybersecurity awareness training to the USG.

Cybersecurity training is required of all USG employees…. If you do not participate, your access to USG information resources may be suspended. Starting in 2020, all USG employees will be required to complete cybersecurity awareness training twice annually, in April and October.

USG IT Handbook

Section 5.9 of the USG IT Handbook addresses organizational responsibilities concerning user awareness training and is part of a larger USG cybersecurity program.

5.9.1 Roles and Responsibilities:

The Chancellor, organization president or chief executive is responsible for ensuring that appropriate and auditable cybersecurity controls are in place to include awareness, training and education.

5.9.2 Discusses learning objectives and training requirements ….

Awareness training shall be conducted biannually, attendance shall be mandatory, completion shall be documented and shall provide practical and simple guidance pertaining to user roles and responsibilities.

Closing Comments

As with all of our documents, they are dynamic and considered works in progress. If you discover an error or have an additional standard or regulation that the community would benefit from mapping, please submit your comment to cybersecurity@usg.edu for correction or consideration.