COMMONWEALTH OF VIRGINIA

Information Technology Resource Management

CYBERSECURITY AWARENESS TRAINING STANDARD

Virginia Information Technologies Agency (VITA)

ITRM Publication Version Control

ITRM Publication Version Control: It is the User's responsibility to ensure they have the latest version of this ITRM publication. Questions should be directed to the VITA's Enterprise Architecture *(EA)* Division. (EA) will issue a Change Notice Alert, post it on the VITA Web site, and provide an e-mail announcement to the Agency Information Technology Resources (AITRs) and Information Security Officers (ISOs) at all state agencies and institutions as well as other parties PPA considers to be interested in the change.

This chart contains a history of this ITRM publication's revisions.

Version	Date	Purpose of Revision
Original	November 1, 2020	Base Document
Revision 1.0	August 31, 2022	Administrative change to improve compliance form (Appendix II) and correct error on core baseline requirements description for "Security of Data".
Revision 1.1	December 8, 2022	Administrative change to correct error on core baseline requirements.

Identifying Changes in This Document

- See the latest entry in the table above
- Vertical lines in the left margin indicate that the paragraph has changes or additions.
- Specific changes in wording are noted using italics and underlines; with italics only indicating new/added language and italics that is underlined indicating language that has changed.

The following examples demonstrate how the reader may identify updates and changes:

Example with no change to text – The text is the same. The text is the same. The text is the same.

Example with revised text – This text is the same. *A wording change, update or clarification has been made in this text.*

Example of new section – *This section of text is new.*

Review Process

Enterprise Solutions and Governance Directorate Review

Online Review

All Commonwealth agencies, stakeholders, and the public were encouraged to provide their comments through the Online Review and Comment Application (ORCA). All comments were carefully evaluated and individuals that provided comments were notified of the action taken.

PREFACE

Publication Designation

ITRM Standard SEC527

Subject

Information Technology Security Awareness Training Standard

Effective Date

January 1, 2021

Compliance Date

January 1, 2021

Supersedes

NA

Scheduled VITA Review:

One (1) year from the effective date, then every two years thereafter.

Authority

Code of Virginia, §2.2-2009
(Additional Powers of the CIO relating to security)

Scope

This standard is applicable to all agencies in the *executive, independent, judicial and legislative branches,* as well as institutions of higher education (collectively referred to as "Agency") that manage, develop, purchase, and use information technology databases or data communications in the Commonwealth. *However, academic* "instruction or research" systems are exempt from this *Standard.* This exemption, does not, however, relieve these academic "instruction or research" systems from meeting the requirements of any other State or Federal Law or Act to which they are subject. This *Standard* is offered only as guidance to local government entities.

Purpose

This standard shall provide a curriculum and materials for training all state employees in information security awareness and in proper procedures for detecting, assessing, reporting, and addressing information security threats.

General Responsibilities

(Italics indicate quote from the Code of Virginia requirements)

Chief Information Officer of the Commonwealth (CIO)

Develops and approves statewide technical and data policies, standards and guidelines for information technology and related systems.

Chief Information Security Officer

The Chief Information Officer (CIO) has designated the Chief Information Security Officer (CISO) to develop Information Security policies, procedures, and standards to protect the confidentiality, integrity, and availability of the Commonwealth of Virginia's information technology systems and data.

Virginia Information Technologies Agency (VITA)

At the direction of the CIO, VITA leads efforts that draft, review and update technical and data policies, standards, and guidelines for information technology and related systems. VITA uses requirements in IT technical and data related policies and standards when establishing contracts, reviewing procurement requests, agency IT projects, budget requests and strategic plans, and when developing and managing IT related services.

Executive Branch Agencies

Provide input and review during the development, adoption and update of statewide technical and data policies, standards and guidelines for information technology and related systems. Comply with the requirements established by COV policies and standards. Apply for exceptions to requirements when necessary.

Judicial, Legislative and Independent Branches

In accordance with the Code of Virginia §2.2-2009 section I: *"This subsection applies to the Commonwealth's executive, legislative, and judicial branches and independent agencies*."

In accordance with the *Code of Virginia* § 2.2-2009, the CIO shall coordinate with and assist state agencies in implementing the annual information security training requirement.

Related ITRM Policies, Standards, and Guidelines

- Commonwealth of Virginia Information Technology Security Standard (ITRM Standard SEC501)

Table of Contents

1. Introduction

1.1 Intent

The intent of this *Security Awareness Training Standard* is to provide agencies with a curriculum and materials developed by the CIO pursuant to subdivision 2 to implement an annual information security training for each of its employees. This Standard has been created based on the requirements in Code of Virginia §2.2-2009-I.

This *Standard* defines the curriculum course requirements that agencies shall implement when creating an annual information security program. State agencies shall develop additional training materials that address specific needs of such agency, provided that such materials do not contradict the training curriculum and materials developed by the CIO.

2. Security Awareness Training Roles and Responsibilities

The roles and responsibilities defined in the *Commonwealth of Virginia Information Technology Security Standard* (ITRM *Standard SEC501*) shall apply to this standard.

2.1 Agency Head

Each Agency Head is responsible for the security of the agency's IT systems and data. Agency heads shall ensure an information security awareness and training program is established.

2.2 Information Security Officer (ISO)

Agency ISOs are responsible to develop and maintain an information security awareness and training program for agency employees and contractors. All IT system users are required to complete IT security awareness and training activities within 30 days of initial employment and by January 31st each year thereafter.

3. Cybersecurity Awareness Training Requirements

3.1 Purpose

The purpose of this curriculum for IT security awareness education is to identify the knowledge areas that are necessary to provide information technology system users in the Commonwealth with appropriate awareness of information systems security requirements and of their responsibilities to identify potential cyber threats and protect the confidentiality, integrity, and availability of information technology resources and systems. The Commonwealth seeks to establish a culture that ensures that all users are working toward a common goal of protecting information, information systems and associated resources.

3.2 Outcome Statement:

This education program is to promote a risk-aware culture and will help ensure that Commonwealth IT system users are able to:

- Demonstrate the safe and secure use of IT system resources
- Understand the need for protection of sensitive information
- Assure the confidentiality of personal information to which they've been entrusted
- Maximize operational effectiveness and increase productivity
- Minimize agency and Commonwealth liability
- Identify potential cyber threats
- Report potential cyber threats in a timely and efficient manner

- Keep compliant with all Commonwealth, regulatory and contractual requirements

3.3 Strategy Framework

Security awareness training should be designed to be flexible and convenient to users' schedules. Agencies shall provide this training using any combination of educational techniques. A list of possible techniques, include, but are not limited to:

- Web-based learning: On-line courses that are accessible 24/7 from any web browser. On-line courses work well for delivering videos, graphics, and activities. They are also frequently self-paced allowing users to proceed to the next level or topic after they have mastered the current step.

- Classroom learning: A traditional instructional method like a classroom lecture works well for many areas of security awareness training. An instructor can incorporate lectures with whiteboards, PowerPoint presentations or other demonstration methods.

- Exercises: This method of teaching gives users a hands-on activity that allows them to participate in a direct and practical type of experience for a particular security area or function. For example, a student could be presented with a simple encryption algorithm and asked to "decrypt" a secret encrypted message.

- Simulation: A simulation activity is similar to an exercise but it offers a more realistic opportunity for the user to participate and learn important skills. One popular type of security awareness simulation is a "phishing exercise." Realistic emails are sent to users to see if they are readily knowledgeable enough to recognize if an email is a "phishing" email and potentially malicious.

- Case Studies: A case study is a method of allowing a student to perform an in-depth and detailed examination of a particular security awareness issue or problem. For example, a student is presented with a scenario that describes a possible illegal or unethical situation. The student must identify the problem and develop a potential solution.

- Gamification: This is a learning technique that includes the elements of game-playing: point scoring, competition with others, rules of play, etc. Gamification is usually more exciting, fun, and engaging to students.

3.4 Verification Methods

It is important that any instructional technique that agencies use include a verification method that assesses that the instruction was effective.

Quizzes are a typical assessment method. Following each instruction, students will be given a quiz or test that demonstrates their understanding of the material. If the material is not understood, the student must repeat the instruction, followed by a new quiz or assessment.

Depending on the instruction method, other types of assessments can be utilized. Group discussions can provide instructors insight into their students' mastery of the material. Students could also be asked to make presentations or develop projects related to the training program.

The main goal is to understand what students know or do not know. When agencies determine that a significant number of students are struggling with particular area or topic of security, agencies should forward that information to VITA, with suggestions for improvement, as part of its certification reporting for annual training compliance.

3.5 Standards Alignment

This curriculum has been developed in accordance with the Code of Virginia, Section 2.2-2009 sub-section I (https://law.lis.virginia.gov/vacode/title2.2/chapter20.1/section2.2-2009/_) which was codified July 1, 2020 with an effective date of January 1, 2021. Sub-section I of 2.2-2009 applies to ***all*** agencies of the Commonwealth's ***executive, independent, legislative and judicial branches***.

Curriculum topics were determined from requirements set forth in the Commonwealth Information Security Standard (ITRM SEC 501 Information Security Standard). The overall requirements for security awareness training are identified in the family of security controls listed in section "AT – Awareness and Training." The control requirements in section AT apply to all employees and contractors of the Commonwealth, including interns or volunteers who use commonwealth IT systems.

In addition, SEC501 identifies additional role-based training requirements. Role-based training is required for all employees and contractors who have been assigned certain roles as part of their duties in support of an agency's IT security program. For example, "System Owners", "Data Owners", "System Administrators", "Information Security Officers" and "Agency Heads" have specific responsibilities related to their respective roles. Agency training shall account for these specialized needs.

The organization must provide 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. On an annual basis or more frequently if necessary.

There are also agencies that need to comply with additional federal, state or contractual regulations. Some of these regulations have their own specific training requirements that need to be addressed. Agencies shall assure that their IT security awareness training program take these regulations into consideration. Examples include but are not limited to the following areas:

- HIPAA (Health Insurance Portability and Accountability Act),
- FTI (Federal Tax Information),
- SSA (Social Security Administration),
- PII (Personally Identifiable Information)
- CJIS (Criminal Justice Information Services).
- FERPA, (Family Education Rights and Privacy Act),
- PHI (Protected Health Information),
- PCI (Payment Credit Card Information) and PCI DSS (Payment Card Industry Data Security Standard)

Agency training shall contain adequate materials for all of their employees or contractors who see or use any information of the types covered by federal, state or contractual regulations.

4. Cybersecurity Curriculum

4.1 Cybersecurity Curriculum Outline

Agencies are required to develop training or procure training for their employees and contractors that meet the objectives of the Cybersecurity Curriculum requirements outlined here:

A. Core Requirements
B. Policy Acceptance and Review
C. Role Based Training
D. Regulatory Training
E. Phishing Exercises

Agencies must develop additional training materials that address the specific needs of the agency if they are not covered in the Cybersecurity Curriculum below (requirement F).

Cybersecurity Curriculum	
Agencies are required to procure, obtain or develop a cybersecurity curriculum that meets all of the requirements identified here: **(A) Core Requirements;** **(B) Policy Review and Acceptance;** **(C) Role Based Training;** **(D) Other Regulatory Requirements;** **(E) Phishing Exercise; and optionally;** **(F) Additional training where required.**	
(A) CORE REQUIREMENTS: *Agencies shall provide cybersecurity awareness training that meets or exceeds all of the core requirements identified here in section A. Any cybersecurity training shall cover the following knowledge areas at a minimum. The specific names of the courses could be different or be combined in other courses depending on the training solution that is chosen, but the knowledge areas below shall be adequately covered.*	
Core Requirements Knowledge Areas	**SEC501 Control**
• **Separation of Duties** - Explains the importance of Control policy according to which no person shall be given responsibility for more than one related function.	**AC-5**
• **Identifying and Reporting Security Incidents** - Prevention and detection of information security incidents, including those caused by malicious code.	**IR-6**
• **Proper disposal of Data Storage Media** – Ensures that retired devices and media have their contents securely removed, destroyed, or overwritten so that it is extremely difficult or impossible to later retrieve data.	**MP-6**
• **Proper Use of Encryption**. This knowledge area explains what encryption is and how an encryption key works to encrypt and decrypt information.	**AT-2, MP-4, SC-8**
• **Access Controls, Secure Passwords** - Creating and changing passwords and the need to keep them confidential.	**AC-2, IA-5**
• **Working Remotely** – Explains how employees can protect themselves by using secure network connections, managing laptop and device security, and following workplace policies to keep themselves and their organization safe.	**AT-17**
• **Intellectual Property Rights** – Explains the different methods for protecting these rights of ownership based on their type.	**AT-2-COV**
• **Security of Data.** Data security is the process of safeguarding digital information throughout its entire life cycle to protect it from corruption, theft, or unauthorized access. It covers everything—hardware,	**PL-4, AC-6, SC-7, 4.1, 4.2**

Cybersecurity Curriculum	
software, storage devices, and user devices; access and administrative controls; and organizations' policies and procedures.	
• **Phishing and Email.** This knowledge area covers key methods cyber attackers use to get people to click on the bait in an email message. It also identifies the primary clues that each person can use to detect phishing, and how to safely check links in email.	**AT-2**
• **Social Engineering.** This knowledge area explains and illustrates different types of social engineering attacks and how people can detect and defend against them.	**AT-2**
• **Least Privilege** – Explains the practice of limiting access rights for users to the bare minimum permissions they need to perform their work.	**AC-2**
• **Privileged Access**. This knowledge area will discuss how privileged users can protect themselves and your organization, including proper use of privileged accounts, limiting the information they share, and how they can detect if a system is compromised.	**AC-1. AC-2**
• **Insider Threat**. This knowledge area will show how to reduce the likelihood of an insider threat attack by using strong organizational security practices.	**SI-4. AT-2**
• **Cloud Services.** This knowledge area will explain the use of cloud services risks to employees and show them how to safely use authorized Cloud providers in your organization.	**AC-20**
• **Browsing Safely**. This knowledge area, staying safe online involves key security behaviors, such as safe browsing, recognizing signs of a security compromise, managing updates, looking for signs of encryption, and logging off websites to remove sensitive information.	**PL-4**
• **Physical Security.** This knowledge area will review how an organization protects its people, property or physical assets from actions and events that can cause losses or damages.	**PE**
• **Hacking.** This knowledge area will focus on the common warning signs used to identify and report an incident, regardless of the cyber-attack employed. It is critical that when any of these signs are observed, they are reported immediately to the help desk or information security team.	**IR-4**
• **Personal Identifiable Information (PII).** This knowledge area will explain what PII is and the extra steps employees must take to protect it and other types of confidential information. Examples include the use of encryption and personal email accounts, the sharing of sensitive information, using only authorized systems to store or process sensitive information, and securely disposing of sensitive data.	**IR-4**
• **Privacy**. This knowledge area provides a basic overview of privacy concepts, setting the stage for additional requirements or standards that apply specifically to your organization.	**AT-2**
• **Social Network.** This knowledge area will review how users can manage the privacy and security settings for social networking applications; how to maintain a positive online reputation; keeping personal information personal and protecting your computer.	**AU-13**
• **Mobile Devices.** How to safely use mobile apps and keep them updated to avoid security issues.	**MP-5**
• **Malware.** This knowledge area will explain what malware is, provides examples of commonly used malware, and covers misconceptions. It will also focus on key methods attackers use to deploy malware and how each of us can defend against them, such as keeping devices updated with current versions of software and security patches for protection and reporting any signs of infection as soon as possible.	**SI-3, SI-4**
• **Ethics.** Ethics will describe challenging situations employees are sometimes confronted with, such as managing unexpected gifts or related conflicts of interest, how to manage uncertain behavior, and knowing when to approach a supervisor or Human Resources with concerns.	**AT-2**
(B) Policy review and acceptance: *Agencies shall require documentation of IT System users' acceptance of the agency's security policies. Cybersecurity awareness training shall include policy review and acceptance for users.*	

Cybersecurity Curriculum	
• **Acceptable Use Policy:** All users of IT systems shall agree to the agency's acceptable use policy.	**AT-2**
• **Remote Access Policy:** All users of IT systems shall agree to the agency's remote access usage and/or Telework Policy**.**	**AT-2**
• **Other Applicable Policies:** Users of IT systems shall review and agree to comply with any applicable agency security policies.	**AT-2**
C) Role Based Training: *Agencies shall provide appropriate cybersecurity training based on the assigned roles and responsibilities of individuals with specific security requirements.*	
• **System Owner Training:** System owners are agency managers responsible for having an IT system operated or maintained. They are responsible for managing system risk, developing policies & procedures for the system. They must maintain compliance with Commonwealth policies and standards.	**2.7, AT-3**
• **Data Owner Training:** Data owners are agency managers responsible for policy and practice decisions regarding data. They are responsible for evaluating and classifying the sensitivity of data; defining data protection requirements; and defining requirements for access to data.	**2.8, AT-3**
• **System Administrator Training:** An administrator is an analyst, engineer or consultant who manages and/or operates a system at the direction of the System Owner, Data Owner or Data Custodian.	**2.9, AT-3**
• **Data Custodian Training:** Data custodians are in physical or logical possession of data. They are responsible for protecting data in their possession and operating systems in a manner consistent with commonwealth policies and standards.	**2.10, AT-3**
• **Agency Head Training:** Agency heads have overall responsibility for the security of the agency's systems and data.	**2.4, AT-2**
(D) Regulatory Training: *Agencies shall provide training for all regulatory or contractual requirements that affect IT users. Agencies need to decide the appropriate level of regulatory training that is required for its users.*	
• **Federal Tax Information (FTI**). This knowledge area explains what federal tax information is and details the steps that must be taken to protect data in order to keep your organization compliant.	**4.2**
• **Health Insurance Portability and Accountability Act (HIPAA).** This knowledge area explains what Federal PII is and the steps people need to take to protect it.	**4.2**
• **Criminal Justice Information Services** (**CJIS)**. This knowledge area explains those requirements, including authorized and unauthorized information sharing, data access, and how to avoid unsafe behaviors.	**4.2**
• **FERPA.** The Family Educational Rights and Privacy Act, also known as FERPA, is a federal law that protects the privacy of student education records. In this updated module, we review the rules and regulations all school faculty, staff, contractors, and student employees should follow when handling student information.	**4.2**
• **Social Security Training (SSA).** The course explains the sensitivity of information and the operational programs of the Social Security Administration for those who will see or access SSA information.	**4.2**
• **Payment Credit Card Information** (**PCI).** If your organization stores, transmits, or processes any cardholder data, it is required to follow PCI DSS. This knowledge area is built on and requires people to watch the Data Security module first as part of compliance training.	**4.2**
• **Federal PII** – Explains how to identify and protect Federal Personally Identifiable information.	**4.2**
• **Personal Health Information** (PHI) This knowledge area describes the importance of PHI, how to identify PHI and why it is important to protect that information.	**IR-4**

Cybersecurity Curriculum	
E) Phishing Exercise: *Phishing refers to email scams that are designed to steal information or identification credentials from users.*	
• **Phishing Exercise:** Agencies are required to conduct a phishing exercise or phishing training with their employee / contractor users. A phishing campaign will help identify if users can successfully recognize, avoid and report phishing attempts.	**AT-2, AT-2-COV**
F) Additional Training (where required): *Agencies shall offer training that goes beyond the required curriculum items when necessary in the agency's environment. The items below are examples of additional training topics for agencies to include when applicable.*	
• **Senior Leadership**. This knowledge area will cover important concepts, such as how to be secure when traveling, proper mobile device use and security, the most common indicators of targeted attacks, and how to set an example to help build a secure culture.	**CM-2. AC-19**
• **New Employee Orientation**. This knowledge area will provide security awareness basics for employees who are new to your organization.	**AT-2**
• **Creating a Cyber Secure Home.** This knowledge area describes the steps that can be used at home to protect personal devices, Wi-Fi networks, and online accounts. It also covers the importance of information backups, such as Cloud services or external hard drives, in the event of an attack, theft, or loss of a device. Secure behaviors at work often start at home.	**CP-9. AC-20. IR-4**

5. Identified Solutions

5.1 Solution Matrix

The matrix provided in Appendix III includes the approved training solutions available and the curriculum requirements they meet. This matrix is intended as a list of training which meets some or all of the curriculum included. A single solution will not meet all of the curriculum requirements and will need to be supplemented with additional solutions or agency training. If an agency would like to use a cybersecurity training solution not listed in the matrix, the agency must obtain approval for the alternative training prior to use (see Appendix I).

Software specifications for any particular training solution often change without notice, so please validate the curriculum requirements are still met prior to performing training at an agency. Refer questions to VITA Commonwealth Security & Risk Management.

See Appendix III for Solution Matrix.

5.2 Security Awareness Training Plans

Agencies must provide their security awareness training plans to VITA annually. The following information is required in the training plan:

- Vendor and software name of solutions used for cybersecurity training purposes.
- Additional information or artifacts documenting the areas the training does not cover.

If an agency's submitted training program is not approved by VITA the agency may resubmit with corrections or propose a remediation plan identifying the steps to address gaps in training. If an agency is unable to meet the standard training requirement, they must submit an exception to VITA.

6. Annual Certification and Reporting for Compliance

6.1 Requirement

Each organization shall:

Annually, by January 31, submit to VITA their proposed annual IT security awareness training plans with appropriate artifacts to VITA for approval (using the form in Appendix I or using a VITA supplied web portal if available).

Use the approved security awareness training for its employees/contractors

Provide employees and contractors agency cybersecurity training *within 30 days of initial employment or contract engagement* and by January 31 of each year thereafter.

Annually submit the following compliance information to VITA (using the table in Appendix II or by web portal when available):

- A certification statement that all employees and contractors have completed required training,
- An evaluation of the efficacy of the cybersecurity training program that the agency provided,
- Any requests for improvement to the curriculum or other aspects of the training program.

Appendix I

VITA Compliance Certification of
Agency Cybersecurity Awareness Training Program

In accordance with the Code of Virginia, Section 2.2-2009 sub-section I, all Commonwealth of Virginia agencies shall report the type of Cybersecurity Awareness Training solution that they will administer to their employees. Training solutions (i.e. software, classroom, or other) are required to meet the curriculum requirements identified in this document.

This information is to be submitted to VITA no later than **January 31, 2021** and every January 31, thereafter.

Please complete the following:

Agency Name: Click or tap here to enter text.

Information Security Officer: Click or tap here to enter text.

Identify Training Solution: please mark your agency's proposed solution to meet the training requirements identified in A, B, C, and D.

		APPROVED SOFTWARE SOLUTIONS *(Agencies who have procured any of these software solutions do not need to change. Agencies that have procured a different software solution or intend to use a different training method, need to let VITA know what it is so that we can evaluate it).*								
		InfoSec	*KnowB4*	*SANS*	*Awareity*	*Security Mentor*	*Other Software	DHRM LMS	Classroom or Other Method	VITA
A	**Core Requirements (required):**									
B	**Policy Review & Acceptance (required):**									
C	**Role Based Training (required):**									
	System Owner Training									
	Data Owner Training									
	System Admin Training									
	Data Custodian Training									
	Agency Head Training									
D	**Regulatory Training (required as needed):**									
	Federal Tax Information (FTI)									
	Health Insurance Portability & Accountability Act (HIPAA)									

	Criminal Justice Information Services (CJIS)									
	FERPA									
	Social Security Training									
	Payment Card Information (PCI)									
	Personal Health Information (PHI)									
E	**Phishing Exercise (required)**									
F	**Additional Training (optional)**									

*If you are planning to use a software solution other than Infosec, KnowB4, SANS, Awareity, or Security Mentor, please indicate it below. Please keep in mind the use of any other training solution must be approved in advance.

Appendix II

Annual Cybersecurity Awareness Training
Verification Compliance Form

In accordance with the Code of Virginia, Section 2.2-2009 sub-section, all Commonwealth of Virginia agencies shall report to VITA the following compliance information below no later than ***January 31st of each year.***

Agency Name: *Click or tap here to enter text.*

Information Security Officer: *Click or tap here to enter text.*

Please complete the following:

1. Provide the number of employees and contractors at your agency: _____
2. How many employees and contractors completed Security Awareness Training: _____
3. Provide a certification statement that all employees and contractors have completed all required training:

Click or tap here to enter text.

4. Provide a reason or justification that all employees/contractors have not completed all training.

Click or tap here to enter text.

5. Provide an evaluation of the efficacy of the cybersecurity-training program that the agency provided

Click or tap here to enter text.

6. Provide any suggestions on how VITA can improve the mandatory curriculum, materials, or any other aspects of the training program.

Click or tap here to enter text.

Appendix III

There are numerous IT security awareness training software solutions available. VITA has identified several that meet the required core curriculum items.

1. Infosec
2. KnowB4
3. Awareity
4. SANS
5. Security Mentor

Any of the five identified training solutions above will meet the "Core Curriculum" requirements of this training standard (requirement A) and the requirement to have users read, review, and accept required security policies (requirement B).

Role-based training (requirement C) can be obtained through the DHRM LMS. Agencies shall use this training or identify/develop other training to meet this requirement.

Most, but not all, regulatory training (requirement D) is available through any of the five identified software training solutions. Agencies shall assure that if it is subject to any particular regulation or contractual requirement that a training solution is selected that addresses those areas. Agencies shall also assure that the training is adequate and in-depth enough for their users.

An annual phishing exercise or campaign is also required (requirement E). Some software solutions may provide this as an optional module or add-on. VITA will facilitate phishing campaigns for agencies as needed.

Agencies shall provide any additional training that is relevant for their users (requirement F).

The use of any other software or solution for training must be approved by VITA in advance. Please let us know what it is that you intend to use and allow us adequate time to review it.

Please note that content in the DHRM LMS changes frequently. In addition, other than role-based training, DHRM LMS content has not been identified or verified as suitable training for this publication. If you plan to use DHRM LMS for training other than role-based training, let us know on the form what courses you found in there that you intend to use so that it can be evaluated and approved.

Solution Matrix: Identified IT Security Training Solutions (An "x" indicates that the requirement can be met)											
A - Curriculum Requirements	**Infosec**	**KnowB4**	**Awareity**	**SANS**	**Security Mentor**	**DHRM LMS**	**VITA**	**Other solution (please identify)**			
Core Requirements	**x**	**x**	**X**	**x**	**x**						
B - Policy Review & Acceptance	**Infosec**	**KnowB4**	**Awareity**	**SANS**	**Security Mentor**	**DHRM LMS**	**VITA**	**Other solution (please identify)**			
Acceptable Use Policy	**x**	**x**	**X**	**x**	**x**						
Remote Access Policy	**x**	**x**	**X**	**x**	**x**						
All Other Applicable Policies	**x**	**x**	**X**	**x**	**x**						
C - Role Based Training	**Infosec**	**KnowB4**	**Awareity**	**SANS**	**Security Mentor**	**DHRM LMS**	**VITA**	**Other solution (please identify)**			
System Owner Training						**x**					
Data Owner Training						**x**					
System Administrator Training					**x**	**x**					
Data Custodian Training						**x**					
Agency Head Training						**x**					
D - Regulatory Training: Agencies shall provide training for any regulatory requirements that affects IT users.	**Infosec**	**KnowB4**	**Awareity**	**SANS**	**Security Mentor**	**DHRM LMS**	**VITA**	**Other solution (please identify)**			
Federal Tax Information (FTI)				**x**							
Health Insurance Portability and Accountability Act (HIPAA)	**x**	**x**	**X**	**x**							
(CJIS) Criminal Justice Information Services	**x**	**x**		**x**							
FERPA	**x**	**x**		**x**							
(SSA) Social Security Training	**x**	**x**									

(PCI) Payment Credit Card Information	x	x	X	x							
Federal PII	x	x	X	x							
PHI – Personal Health Information	x	x	X	x							
E – Phishing Exercise	**Infosec**	**KnowB4**	**Awareity**	**SANS**	**Security Mentor**	**DHRM LMS**	**VITA**	**Other solution (please identify)**			
An annual phishing campaign or exercise is required. Some software provides this as an optional module or VITA will facilitate this for your agency.					x		x				
F - Additional Training (where required). Please substitute additional training that you think is appropriate at your agency.	**Infosec**	**KnowB4**	**Awareity**	**SANS**	**Security Mentor**	**DHRM LMS**	**VITA**	**Other solution (please identify)**			
Senior Leadership	x	x		x							
New Employee Orientation	x	x		x							
Creating a Secure Cyber Home				x	x						

Note: This matrix is subject to change. Other identified solutions will be added at future dates.