CyberSecurity- Incident Response & Reporting

Target Audience: The audience is all EPA employees, contractors, and all other users of EPA information and information systems that support the operations and assets of the EPA.

Learning Objectives: By the end of the training, the learners will be able to…

- Recognize Controlled Unclassified Information (CUI), PII, and Sensitive Personally Identifiable Information (SPII).
- Recognize types of security incidents,
- Identify the process to report and respond to security incidents, and
- Identify your security contacts.

Seat Time: 45 minutes

Outline:

- Course Intro / Navigation / Objectives

- Privacy Basics
  - Security acronyms and abbreviations
    - PII- Personally Identifiable Information
    - SPII- Sensitive Personally Identifiable Information
    - CUI- Controlled Unclassified Information
    - CSIRC- Computer Security Incident Response Capability
    - ISO- Information Security Officer
- Knowledge Check
- Types of Security Incidents
  - Confidential/Unencrypted
  - Virus, Phishing & Attacks
  - Loss, Damage & Theft
  - Unauthorized Person Use

- Response & Reporting
  - 5 steps to report and respond to a security incident.
    - Stop
    - Call - Security Contacts
    - Email
    - Document
    - Follow-Up
- Scenario: Responding to a Security Incident
  - Scene will show an employee panicking due to a computer being hacked. A coworker comes in to guide her through the appropriate steps to responding and reporting the system hack.
- Summary
- Quiz
- Congratulations

Directions:

1. Be specific: When providing feedback, be as specific as possible. Instead of saying something like, "I don't like it," provide specific details about what you don't like and why. This will help the team understand your concerns and make the necessary changes.
2. Focus on the objectives: Keep the project objectives in mind when providing feedback. Ask yourself whether the proposed solution is meeting the objectives and how it can be improved. Provide feedback on what is and isn't working in relation to the project goals.
3. Be constructive: Feedback should be constructive and focused on improvement. Avoid being overly critical or negative. Instead, focus on providing actionable feedback that will help the team make progress.
4. Provide feedback in a timely manner: Feedback is most effective when it is provided in a timely manner. Don't wait until the last minute to provide feedback, as this can delay the project and make it more difficult to make changes.
5. Use clear language: Use clear and concise language when providing feedback. Avoid using technical jargon or complex language that may be difficult for the team to understand. Be straightforward and direct in your feedback.
6. Consider the audience: Consider who will be receiving your feedback and tailor it accordingly. For example, if you're providing feedback to a designer, you may want to focus on visual elements such as color, layout, and typography.

7. Provide examples: Providing examples can help clarify your feedback and make it more actionable. Use examples of what you do and don't like, and explain why. This can help the team understand your perspective and make the necessary changes.

By following these instructions, you can provide effective feedback that will help the team make progress and achieve the project objectives.

- Throughout this document, the correct answers for all assessment questions are in **bold** text.

Module Resources/References:

Slide [1.1]/ Menu Title: *Welcome*			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
No top/bottom border Background image: Photographic image of persons hand holding a cell phone to open an security application Course title set in semitransparent shape overlaying the background image Custom Start and Navigation buttons	[Slide Title] **Introducing Incident Response & Reporting** [Buttons] START NAVIGATION	Welcome to the Information Security eLearning course. In this course, you will learn about incident response and reporting. If you experience a security incident, you should know what to do immediately, and who to contact. If you would like some guidance with navigating the course, click the Navigation lock. If you are familiar with the course navigation player, click the objectives lock button to begin. When you're ready, let's get started.	The Start and Navigation buttons will fade in timed with the VO reference The Start button will jump to slide 1.3 The Navigation button will jump to the next slide (slide 1.2)
Notes:			

Slide [1.2]/ Menu Title: *Navigation*			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Player shows the Menu on the left. Background image: Photo of compass on half on the screen; white space on the other half Caption bubbles with labels point to player features	[Slide Title] **Navigation** [Directions] Take a moment to review the course player so you feel comfortable navigating through the course. If you know your way around, you may proceed to the next slide. [Captions] Next Previous Volume Replay Progress bar Play/Pause	Please take a moment to review the course player so you feel comfortable navigating through the course. If you know your way around, you may proceed to the next slide. The progress bar shows where you are in the narration. You can start, stop, and replay the audio as needed. There are Previous and Next buttons next to the progress bar, along with the audio volume. You must listen to the whole narration before you can continue. Click the next button now to begin the course.	Caption bubbles with text labels will fade in timed with their reference in the audio.
Notes:			

Slide [1.3]/ Menu Title: *Learning Objectives*

Visual / Display:	Slide Text:	Narration / Voiceover:	Animation / Interaction:
Background image: Photo of office space on half on the screen; white space on the other half for slide text	[Slide Title] **Learning Objectives** 1. Recognize types of security incidents, 2. Identify the process to report and respond to security incidents, and 3. Identify your security contacts.	By the time we finish, you'll know how to: Recognize types of security incidents, Identify the process to report and respond to security incidents, and Identify your security contacts. Click on the next button to learn more.	On the left side of the screen, the learning objectives text will fade in timed with the VO.

Notes:

Slide [1.4]/ Menu Title: *Privacy Basics*   Objective: [#]

Visual / Display:	Slide Text:	Narration / Voiceover:	Animation / Interaction:
Background image: Photo of office space with workers on the center on the slide with rounded and soft edge border	[Slide Title] **InfoSec. & Privacy Basics** [Top Lock Icon]	The purpose of Information Security and Privacy are to protect and manage the confidentiality, integrity and availability of information and information systems.	This is the home slide for a branching to three slides, one for each lock shown on the

effect; white space on ⅓ of screen for slide text Direction slide text appears above the locks on the right side of the screen to the right of the title. On the right are three vertical locks arranged top to bottom that take up most of the remaining space Each lock is labeled with a title inside the rectangle.	PII [Middle Lock Icon] SPII [Bottom Lock Icon] CUI [Directions] Click on each lock to learn more about the security acronyms.	Click on each lock to learn more about the security acronyms.	screen. The lock will act as custom buttons. When the learner clicks each one, they will jump to the corresponding slide. PII Button – Jumps to 1.5 SPII Button – Jumps to 1.6 CUI Button – Jumps to 1.7 The Next button in the player will be hidden from the learner until all three rectangles are selected and therefore all three branching slides are visited. The learner will be returned to this home slide after visiting each slide linked to each of the three locks. The locks will have visited states so when the learner returns to this home slide, it is clear which rectangle they've already viewed.

			The three locks are restricted to the learner until the Narrator VO ends. Once the buttons are released, the learner will be able to click on them in any order
			Once the learner views the three slides that branch from this one, the Next button will be displayed.
			The Next button will jump to Slide 1.8.

Notes:

Slide [1.5]/ Menu Title: *PII*			Objective: [#]
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Same office space as slide 1.4 with green transparent film over picture, so appears as if we are diving deeper into the new content The same lock used for the button on the home slide (title and icon) now appears grayed indicating to	[Slide Title] **PII** [Subtitle] Personally Identifiable Information ● your name ● Social Security number	PII stands for Personally Identifiable Information The federal government restricts unauthorized disclosure of your PII. Types of PII include: your name, Social Security number, driver's license, citizenship, gender, birth date, place of birth, and various other types of information that can be used to identify you. It is your	Slide text fades in with bullet points timed with the VO reference. The directions badge glides in using a motion path to instruct

the learner selected the specific lock Direction slide text appears above the rectangle on the right side of the screen to the right of the title (in the solid-colored badge.)	● driver's license ● citizenship ● gender ● birth date ● place of birth [Directions] Click next to continue.	responsibility to safeguard your PII. Be careful not to disclose your PII to any individual or make it available anywhere without your written consent.	the learner to click on the next button to continue. Next button is disabled until just before the timeline ends. Next button returns learner to home slide (Slide 1.4)
Notes:			

Slide [1.6]/ Menu Title: *SPII*			Objective: [#]
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Same office space as slide 1.4 with green transparent film over picture, so appears as if we are diving deeper into the new content The same lock used for the button on the home slide (title and icon) now appears grayed indicating to the learner selected the specific lock Direction slide text appears above the rectangle on the right side of the screen to the right of the title (in the solid-colored badge.)	[Slide Title] **SPII** [Subtitle] Sensitive Personally Identifiable Information There are 3 categories of PII classified as sensitive: Category 1 Sensitive PII consists of Social Security number, Drivers license, State Identification number, Passport number, Alien registration number, Biometric identifiers. Category 2 Sensitive PII	SPII stands for sensitive personally identifiable information. SPII is a subset of PII that should not be made public. If your SPII is lost, compromised, or disclosed without authorization, you could experience substantial harm, embarrassment, inconvenience, or unfairness. There are 3 categories of PII classified as sensitive. Category 1 Sensitive PII consists of Social Security number, Drivers license, State Identification number, Passport number, Alien registration number, Biometric identifiers. Category 2 Sensitive PII are Any medical information associated with an individual. Category 3 Sensitive PII are financial account information associated with an individual.	Slide text fades in with bullet points timed with the VO reference. Slide text fades in with each category timed with VO reference. (Text should come in 3 rounds where "Category 2" replaces the space that "Category 1" had taken once it fades out.) The directions badge glides in using a motion path to instruct

	are Any medical information associated with an individual. Category 3 Sensitive PII are financial account information associated with an individual.		the learner to click on the next button to continue. Next button is disabled until just before the timeline ends. Next button returns learner to home slide (Slide 1.4)

Notes:

Slide [1.7]/ Menu Title: *CUI*			Objective: [#]
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Same office space as slide 1.4 with green transparent film over picture, so appears as if we are diving deeper into the new content The same lock used for the button on the home slide (title and icon) now appears grayed indicating to the learner selected the specific lock Direction slide text appears above the rectangle on the right side of the screen to the right of the title (in the solid-colored badge.)	[Slide Title] **CUI** [Subtitle] Controlled Unclassified Information ● Controlled technical information with military or space application. ● Protected critical energy infrastructure information, including nuclear reactors and materials.	CUI stands for Controlled Unclassified Information , formally known as Sensitive But Unclassified. It is information that has a degree of confidentiality that, if lost, misused, accessed without authorization or modified, its confidentiality could be compromised and adversely affect national interests, the operation of X, or you. CUI consist of Controlled technical information with military or space application. Protected critical energy infrastructure information, including nuclear reactors and materials. Export control information or materials. Geodetic and geospatial information related to imagery intelligence.	Slide text fades in with bullet points timed with the VO reference. The directions badge glides in using a motion path to instruct the learner to click on the next button to continue. Next button is disabled until just before the timeline ends. Next button returns learner to home slide (Slide 1.4)

	● Export control information or materials. ● Geodetic and geospatial information related to imagery intelligence.		

Notes:

Visual / Display:	Slide Text:	Narration / Voiceover:	Animation / Interaction:
[Same Visual Design as 1.4] Background image: Photo of office space with workers on the center on the slide with rounded and soft edge border effect; white space on ⅓ of screen for slide text Direction slide text appears above the locks on the right side of the screen to the right of the title.	[Slide Title] **InfoSec. & Privacy Basics** [Top Lock Icon] CSIRC [Bottom Lock Icon] ISO [Directions] Click on each lock to learn more about the security acronyms.	Click on each lock to learn more about the security acronyms.	This is the home slide for a branching to two slides, one for each lock shown on the screen. The lock will act as custom buttons. When the learner clicks each one, they will jump to the corresponding slide. CSIRC Button – Jumps to 1.9 ISO Button – Jumps to 1.10

On the right are three vertical locks arranged top to bottom that take up most of the remaining space Each lock is labeled with a title inside the rectangle.			The Next button in the player will be hidden from the learner until all three rectangles are selected and therefore all three branching slides are visited. The learner will be returned to this home slide after visiting each slide linked to each of the three locks. The locks will have visited states so when the learner returns to this home slide, it is clear which rectangle they've already viewed. The three locks are restricted to the learner until the Narrator VO ends. Once the buttons are released, the learner will be able to click on them in any order Once the learner views the three slides that branch from this one, the Next button will be displayed.

			The Next button will jump to Slide 1.11.
Notes:			

Slide [1.9]/ Menu Title: *CSIRC*			Objective: [#]
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Same design as slide 1.5/6/7 with green transparent film over picture, so appears as if we are diving deeper into the new content The same lock used for the button on the home slide (title and icon) now appears grayed indicating to the learner selected the specific lock Direction slide text appears above the rectangle on the right side of the screen to the right of the title (in the solid-colored badge.)	[Slide Title] **CSIRC** [Subtitle] Computer Security Incident Response Capability CSIRC efforts provide agencies with a centralized and cost-effective approach to handling computer security incidents so that future problems can be efficiently resolved and prevented.	CSIRC stands for Computer Security Incident Response Capability. CSIRC efforts provide agencies with a centralized and cost-effective approach to handling computer security incidents so that future problems can be efficiently resolved and prevented.	Slide text fades in with bullet points timed with the VO reference. The directions badge glides in using a motion path to instruct the learner to click on the next button to continue. Next button is disabled until just before the timeline ends. Next button returns learner to home slide (Slide 1.8)
Notes:			

Slide [1.10]/ Menu Title: *ISO*			Objective: [#]
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Same design as slide 1.5/6/7 with green transparent film over picture, so appears as if we are diving deeper into the new content The same lock used for the button on the home slide (title and icon) now appears grayed indicating to the learner selected the specific lock Direction slide text appears above the rectangle on the right side of the screen to the right of the title (in the solid-colored badge.)	[Slide Title] **ISO** [Subtitle] Information Security Officer An Information Security Officer (ISO) is the person inside every state agency who has the explicit authority and duty to administer information security requirements.	ISO stands for Information Security Officer. ISO is the person inside every state agency who has the explicit authority and duty to administer information security requirements.	Slide text fades in with bullet points timed with the VO reference. The directions badge glides in using a motion path to instruct the learner to click on the next button to continue. Next button is disabled until just before the timeline ends. Next button returns learner to home slide (Slide 1.8)
Notes:			

Slide [1.11]/ Menu Title: Types of Security Incidents			Objective: [#]
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Background image: Photo of security camera takes up the entire screen	[Slide Title] **Types of Security Incidents** [Incident Definition]	**Types of Security Incidents** An incident refers to any violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices – all of	Slide text fades in with bullet points timed with the VO reference.

Slide [1.11]/ Menu Title: Types of Security Incidents			Objective: [#]
Directions badge appears at the top on the right side of the screen to the right of the title. List of incidents displayed in a unique format	An incident refers to any violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices – all of which can compromise your information or information systems you use. [Types of Security Incidents] ● Confidential/Un encrypted ● Virus, Phishing & Attacks ● Loss, Damage & Theft ● Unauthorized Person Use	which can compromise your information or information systems you use. Today's high-speed Internet connections can allow an adversary to steal gigabytes of your or X's data in seconds! Since every second counts when it comes to reporting security incidents, failing to report immediately allows the hacker more time to operate unnoticed in the X network. It is your responsibility to report incidents as soon as you identify them. So stay alert – your quick response can prevent a breach. Here are four common incidents types: confidential/unencrypted, virus, phishing & attacks, loss, damage & theft, and unauthorized person use. Here are 4 common incident types: ● Confidential/Unencrypted ● Virus, Phishing & Attacks ● Loss, Damage & Theft ● Unauthorized Person Use	Incident definition fades in and out with VO. 2 Gifs relating to content fades in and out with VO. Slide returns to image of security camera Types of incident listed with VO. The directions badge glides in using a motion path to instruct the learner to click on the next button to continue. Next button is disabled until the learner clicks on each type of incident. Next button jumps learner to (Slide 1.12)
Notes:			

Slide [1.11a]/ Menu Title:			Objective: [#]
Visual / Display:	Slide Text:	Narration / Voiceover:	Animation / Interaction:

Visual / Display:	Slide Text:	Narration / Voiceover:	Animation / Interaction:
Background image: Photo that relates to each individual type of security incident Black transparent text box with white font Number of type on top corner of text box An "x" to close out the slide	[Slide title] Confidential/Unencrypted [Slide text] Accidentally sending a report containing confidential PII, SPII, and other CUI to a person not authorized to view the report, or sending it unencrypted.	Incident 1 Confidential or Unencrypted Accidentally sending a report containing confidential PII, SPII, and other CUI to a person not authorized to view the report, or sending it unencrypted.	Slide text fades in with bullet points timed with the VO reference. Next button is disabled until the learner clicks on each type of incident. "X" jumps learner back to home slide

Notes:

Slide [1.11b]/ Menu Title: **Objective: [#]**

Visual / Display:	Slide Text:	Narration / Voiceover:	Animation / Interaction:
Background image: Photo that relates to each individual type of security incident Black transparent text box with white font Number of type on top corner of text box An "x" to close out the slide	[Slide title] Virus, Phishing & Attacks [Slide text] Any security situation that could compromise X information or information systems (e.g., virus, phishing email, social engineering attack).	Incident 2 Virus, Phishing & Attacks Any security situation that could compromise X information or information systems (e.g., virus, phishing email, social engineering attack).	Slide text fades in with bullet points timed with the VO reference. Next button is disabled until the learner clicks on each type of incident. "X" jumps learner back to home slide

Notes:

Slide [1.11c]/ Menu Title: **Objective: [#]**

Visual / Display:	Slide Text:	Narration / Voiceover:	Animation / Interaction:
Background image: Photo that relates to each individual type of security incident Black transparent text box with white font Number of type on top corner of text box An "x" to close out the slide	[Slide title] Loss, Damage & Theft [Slide text] Loss, damage, or theft of equipment, media, or documents containing PII, SPII, and other CUI.	Incident 3 Loss, Damage & Theft Loss, damage, or theft of equipment, media, or documents containing PII, SPII, and other CUI.	Slide text fades in with bullet points timed with the VO reference. Next button is disabled until the learner clicks on each type of incident. "X" jumps learner back to home slide
Notes:			

Slide [1.11d]/ Menu Title:			Objective: [#]
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Background image: Photo that relates to each individual type of security incident Black transparent text box with white font Number of type on top corner of text box An "x" to close out the slide	[Slide title] Unauthorized Person Use [Slide text] Allowing an unauthorized person to use your computer or credentials to access CUI.	Incident 4 Unauthorized Person Use Allowing an unauthorized person to use your computer or credentials to access CUI.	Slide text fades in with bullet points timed with the VO reference. Next button is disabled until the learner clicks on each type of incident. "X" jumps learner back to home slide
Notes:			

Slide [1.12]/ Menu Title: Knowledge Check			Objective: [#]
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Background image: Office space takes up the entire slide The question text appears larger than the content options, which are displayed below the question. All text has a transparent background; blue text for descriptions; white text for acronyms	[Slide Title] **What is the difference between the listed InfoSec. Personnel & Policy?** [Directions] Drag the items into the boxes on the right to match their descriptions. [Answer Choices] ● Efforts provide agencies with a centralized and cost-effective approach to handling computer security incidents so that future problems can be efficiently resolved and prevented. **[CSIRC]**	Drag the items into the boxes on the right to match their descriptions. Click the submit button when you are finished.	This slide is a drag-and-drop interaction. There will be 4 phrases as drag items that the learner will need to sort between the four drop targets matching their descrptions. They will be set in rectangles of one of the palette colors. The drag items should appear in a scrambled order so they are not already sorted by type of privacy. Score by question with 2 attempts.

	- Information has a degree of confidentiality, if lost, misused, accessed without authorization or modified, its confidentiality could be compromised and adversely affect national interests. **[CUI]** - The person inside every state agency who has the explicit authority and duty to administer information security requirements. **[ISO]** - Types of information include: your name, Social Security number, driver's license,		

	citizenship, gender, birth date, place of birth, etc. **[PII]**		
Notes:			

Slide [1.12a]/ Menu Title:			Objective: [#]
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Green square covers half on the slide. The buttons are clearly displayed. Try not to cover Drag and Drop interaction (if possible).	[Slide Title] **Correct** [Directions] That's right! You selected the correct response. [buttons] Continue	That's right! You selected the correct response.	The Continue button jumps to Slide 1.14
Notes:			

Slide [1.12b and 1.12c]/ Menu Title:			Objective: [#]
Visual / Display:	Slide Text:	Narration / Voiceover:	Animation / Interaction:
Red square covers half on the slide. The buttons are clearly displayed. Try not to cover Drag and Drop interaction (if possible).	[Slide Title] **Incorrect** [Directions] You did not select the correct response. [buttons] Continue Review [Slide Title (Try Again)] **Incorrect** [Directions]	You did not select the correct response. Use this time to refresh your understanding of the different security acronyms or continue. [Try Again] This layer does not have narration.	The Continue button jumps to Slide 1.14 The Review button jumps to Slide 1.13

	That is incorrect. Please try again. [buttons] Try Again		
Notes:			

Visual / Display:	Slide Text:	Narration / Voiceover:	Animation / Interaction:

Nearly the entire slide is taken up by an accordion interaction. An accordion interaction is similar to a tab "click to reveal" interaction except the tabs are vertical like an accordion.
 	
Four tabs displaying the tab titles takes up about 1/3-1/4 of the accordion area, and are shown vertically, leaving the remainder
	[Slide Title]
	
	InfoSec. & Privacy Review
	
	[Numbered Tabs]
	  1. PII
	  2. CUI
	  3. CSIRC
	  4. ISO
		Okay, let's take another look at the different exampleS/descriptions of PII, CUI, CSIRC, ISO. You'll get it!
		
		Click on each tab to learn more, then click next when you are finished.
		
		[Adjust this direction if necessary to ensure learner understands how to
			The Next button will be restricted until all 4 of the tabs have been selected and all 4 layers have been viewed.
			
			When the learner clicks on the Next button, it will jump to Slide 1.14

		interact with the accordion based on how it is developed.]	
space for content to show within the accordion frame. The closed accordion will show on the screen to start. Background image: office space with workers on the center on the slide with rounded and soft edge border effect When the learner clicks on each tab, it will pop to its open position and display the information for that tab. Each tab should be a different palette color. The layer associated with each tab, and therefore the "open" section of each accordion area should have the same background palette color as the tab for that section.	[Directions, shown on closed accordion. Adjust this direction if necessary to ensure learner understands how to interact with the accordion based on how it is developed.] Select each tab to learn more.		
Notes:			

Slide [1.13a]/ Menu Title:			Objective: [#]
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Unique image related to tab content shown on the entire slide within open accordion. Text is centered on the image. Subtitle displayed prominently within open section of accordion. Bullet points listed below.	[Subtitle] **PII** Definition: Any type of personal information that identifies an individual Examples: First and last name Email address Home address Phone number Photo of a person's face A person's voice or fingerprint	N/A	Learner can select another tab from this layer or be automatically brought back to the base layer to select a new tab, depending on how the accordion interaction is developed.
Notes:			

Slide [1.13b]/ Menu Title:			Objective: [#]
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**

Visual / Display:	Slide Text:	Narration / Voiceover:	Animation / Interaction:
Unique image related to tab content shown on the entire slide within open accordion. Text is centered on the image. Subtitle displayed prominently within open section of accordion. Bullet points listed below.	[Subtitle] **CUI** Definition: Any sensitive personally identifiable information with a greater chance of causing harm if compromised or misused Examples: Credit card information Account credentials Account recovery information Health information Voice, fingerprint, or photo of a person's face if used with recognition software	N/A	Learner can select another tab from this layer or be automatically brought back to the base layer to select a new tab, depending on how the accordion interaction is developed.

Notes:

		N/A	
Unique image related to tab content shown on the entire slide within open accordion. Text is centered on the image.

Subtitle displayed prominently within open section of accordion. Bullet points listed below. | [Subtitle]

CSIRC

Incidents involving these threats, including computer viruses, malicious user activity, and vulnerabilities associated with high technology, require a skilled and rapid response before they can cause significant damage. These increased computer security efforts, described here as Computer Security Incident Response Capabilities (CSIRCs), have as a primary focus the goal of reacting quickly and efficiently to computer security incidents. | | Learner can select another tab from this layer or be automatically brought back to the base layer to select a new tab, depending on how the accordion interaction is developed. |
| **Notes:** | | | |

Slide [1.13d]/ Menu Title:			Objective: [#]
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Unique image related to tab content shown on the entire slide within open accordion. Text is centered on the image. Subtitle displayed prominently within open section of accordion. Bullet points listed below.	[Subtitle] **ISO** An Information Security Officer (ISO) is the person inside every state agency who has the explicit authority and duty to administer information security requirements.	N/A	Learner can select another tab from this layer or be automatically brought back to the base layer to select a new tab, depending on how the accordion interaction is developed.
Notes:			

Slide [1.14]/ Menu Title: Reporting & Responding			Objective: [#]
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Background image: Tech support in space on the center on the slide with rounded and soft edge border effect; Steps listed out horizontally	[Slide title] **Reporting & Responding Steps** 1. Stop 2. Call	If you suspect that a computer security, confidential information disclosure, or PII incident has occurred or is occurring, you must react quickly and say something about it.	Direction slide text appears on the right side of the screen to the right of the title (in the solid-colored badge.)

	3. Email 4. Write 5. Follow-Up [Directions] Click on each step to learn more.	Click on each step to learn more.	Restrict learn from clicking on steps out of order.

Notes:

Slide [1.14a, 1.14b, 1.14c, 1.14d, 1.14e]/ Menu Title:			Objective: [#]
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Background image: (Grayed out to show as layers) Tech support in space on the center on the slide with rounded and soft edge border effect; Steps listed out horizontally Callout shapes for each step. Each layer highlights the individual listed step at the bottom so learners know which step they are on. Apply photo on specific steps that have longer VO audio.	[Step 1 (1.14a)] **Stop everything!** ● Do not try to fix the problem or stop the attack yourself. ● Do not turn off the affected system(s). ● Do not use or allow others to use the affected system, except for incident responders. ● Do not share removable media. [Step 2 (1.14b)] **Call the X Call Center**	[Step 1] If you suspect that computer security, confidential information, or PII incident has occurred or is occurring, you need to stop everything! Do not try to fix the problem or stop the attack yourself. Do not turn off the affected system(s). Do not use or allow others to use the affected system, except for incident responders. Do not share removable media. [Step 2] Next, call your ISO and the X Call Center immediately to report it!Follow all instructions provided by the X Helpdesk and X incident responders. [Step 3] If you experience an incident such as data breaches and spillage (especially of PII,	Slide text/images fades in timed with the VO reference. Callout shapes transitions in for each step. Each layer highlights the individual listed step at the bottom so learners know which step they are on. The Next button will be restricted until all 4 of the tabs have been selected and all 4 layers have been viewed. When the learner clicks on the Next button, it will jump to Slide 1.14

| | Call your ISO and the X Call Center immediately to report it!
[Step 3 (1.14c)]
Send Mitigating Email
    ● The email and data in question should be deleted from your email folder and removed from the recycle bin.
    ● Your Privacy Official or the CSIRC will direct you as to what messages you should send in response to an incident.
[Step 4 (1.14d)]
Write down information
    ● The date/time of the incident,
    ● What you were doing at the time you first noticed the suspicious activity,
    ● What you observed, and | SPII, and other CUI), you need to follow X policy and send a mitigating email to the same recipients of the original breached email or data spill.
The email and data in question should be deleted from your email folder and removed from the recycle bin.
Your Privacy Official or the CSIRC will direct you as to what messages you should send in response to an incident.

[Step 4]
If anything suspicious occurs, you should document what you experience.
Immediately write down any information that may be helpful to investigators, such as:
The date/time of the incident,
What you were doing at the time you first noticed the suspicious activity,
What you observed, and
Names of others who may have observed the same suspicious activity.

[Step 5]
Following an incident, you should not use the affected systems until you are told that it is OK to do so by the X CSIRC, your ISO, or your manager.
Your manager and ISO are to review any and all incidents, and will follow up on open tickets and reports provided by the X CSIRC in order to improve recovery efforts. They also will disseminate | |

	Names of others who may have observed the same suspicious activity. [Step 5 (1.14d)] **Incident Recovery Follow-Up** Do not use the affected systems until you are told that it is OK to do so by the X CSIRC, your ISO, or your manager.	information as necessary and appropriate to you and your coworkers to increase information security and privacy awareness.	

Notes:

Slide [1.15]/ Menu Title: Scenario			Objective: [#]
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Background image: Casual office space with hallway This slide begins with the avatar of Kris (software developer) on the right side of the slide facing across the hall. Marcus avatar will enter on the left side of the slide facing right. The two avatars are centered.	[Slide title] **Workplace Scenario** [Kris caption] Oh no! My documents… [Marcus caption]	Let's take a look at a real life example. [Kris caption] Oh no! My documents… [Marcus caption] Kris, what's wrong? [Kris caption]	The thought and caption text will be displayed on the slide timed with the VO audio.

Caption bubbles (speech bubbles) track Kris's thoughts and their conversation on screen. As Marcus and Kris converse, the caption shape will remain between them.

Kris avatar has 4 poses: frustrated, conversing, on the phone, thinking/listening

Marcus avatar has 4 poses: concerend, conversing (to Kris), conversing (to learner) | Kris, what's wrong?

[Kris caption]

My files are being removed from my computer! I think I'm being hacked. I clicked on a link from an email. I thought…

[Marcus caption]

Stop! Quick! Call your ISO and the X Call Center.

[Directions]

Click on the phone to see what happens next. | My files are being removed from my computer! I think I'm being hacked. I clicked on a link from an email. I thought…

[Marcus caption]

Stop! Quick! Call your ISO and the X Call Center.

[Directions]

Click on the phone to see what happens next. | Slide begins with Kris entering the office setting thinking aloud to herself.

Marcus then appears on the left facing right.

Caption bubbles track their conversation, with slide text fading in and out on time timeline, timed with the VO

When VO directs the learner to click on the phone, a hotspot on the phone will trigger jumping to the next slide.

Directions to click on the phone will fade in with the VO.

The Next button will be hidden on this slide. |

Notes:			

Slide [1.15a]/ Menu Title:			**Objective: [#]**
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Background image: Casual office space This slide begins with the avatar of Kris (on the phone) on the right side of the slide facing the learner. Marcus avatar will enter on the left side of the slide facing right. The two avatars are centered. Caption bubbles (speech bubbles) track Kris's thoughts and their conversation on screen. As Marcus and Kris converse, the caption shape will remain between them. Kris avatar has 4 poses: frustrated, conversing, on the phone, thinking/listening	[Kris caption] Got it! Im on hold now. [Marcus caption] You also need to send a mitigating email to the recipient of the email. Be sure to write everything down for the investigators. The date, time, what you observed… [Kris caption] Okay, I'll do that while I wait for a representative. How long do you think this will take? I have a deadline coming up.	[Kris caption] Got it! Im on hold now. [Marcus caption] You also need to send a mitigating email to the recipient of the email. Be sure to write everything down for the investigators. The date, time, what you observed… [Kris caption] Okay, I'll do that while I wait for a representative. How long do you think this will take? I have a deadline coming up. [Marcus caption] Following an incident, you should not use the affected systems until you are told	The thought and caption text will be displayed on the slide timed with the VO audio. Marcus slides in on the left facing right. Caption bubbles track their conversation, with slide text fading in and out on time timeline, timed with the VO. The Next button will be normal on this slide after the VO has ended.

| Marcus avatar has 4 poses: concerned, conversing (to Kris), conversing (to learner) | [Marcus caption]

Following an incident, you should not use the affected systems until you are told that it is okay to do so by the X CSIRC, your ISO, or your manager. Your manager and ISO are to review any and all incidents, and will follow up on open tickets and reports provided by the X CSIRC in order to improve recovery efforts.

Getting to the root of your problem and tackling it quickly saves system information from theft or damage, You'll be up and running in no time. | that it is okay to do so by the X CSIRC, your ISO, or your manager. Your manager and ISO are to review any and all incidents, and will follow up on open tickets and reports provided by the X CSIRC in order to improve recovery efforts.

Getting to the root of your problem and tackling it quickly saves system information from theft or damage, You'll be up and running in no time. | |

Notes:

Slide [1.16]/ Menu Title: Summary			Objective: [#]
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**

Same background image as Welcome Slide (1.1): Photographic image of persons hand holding a cell phone to open an security application Slide title set in semitransparent shape overlaying the background image Each bullet set in rectangles to form a squared group	[Slide Title] Summary In this module you learned about: ● Recognizing Controlled Unclassified Information (CUI), PII, and Sensitive Personally Identifiable Information (SPII). ● Recognizing types of security incidents, ● Identifying the process to report and respond to security incidents, and ● Identifying your security contacts. s	Let's summarize what you learned in this module. What is an incident? Four types of incidents. Actions to take if an incident occurs. Incident response, recovery, and security contacts.	Four rectangles fly in from each corner of the slide. Slide text/rectangles slide in and timed with the VO reference. Next button is disabled until just before the timeline ends.
Notes:			

Slide [1.17]/ Menu Title: Assessment			Objective: [#]
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Background image:

Photo of office space on right half of the slide; text appear the left side of the screen. | [Slide Title]
Assessment

The quiz consists of 5 questions. You must get 80% correct to pass the assessment.

Click Next to begin. | It's time for your assessment. You'll answer 5 questions. You must earn 80% to pass.
When you're ready, click next to begin. | |
| **Notes:** | | | |

Slide [1.18]/ Menu Title: #1 QA			Objective: [#]
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
All 5 assessment question slides should have the same layout and formatting.

Background image:

Office space takes up the entire slide | [Slide Title]

Question #1

[Question]

Along with the ISO, who else should you call if you suspect you have experienced a security breach or incident? | Select the best answer choice and click the submit when you are finished.

Along with the ISO, who else should you call if you suspect you have experienced a security breach or incident? | Score by question with 1 attempt for each quiz question as the learner progresses through the quiz. They will be able to Retake the entire quiz at the end if they do not pass.

Results slide 1.23; graded quiz slide – multiple choice. |

The question number text appears larger than the multiple choice answer options, which are displayed below the question. All text has a transparent background; white text	[Answer Choices] 1. **The X Call Center** 2. McAfee 3. The NSA 4. Norton Security		When learner clicks Submit, submit multiple choice and advance to next slide. The learner should not get *immediate* feedback with Correct or Incorrect feedback layers. They should answer all of the questions sequentially FIRST in the graded assessment, then receive their score on the Results page. If they do not pass, they can come back and review the quiz.
Notes:			

Slide [1.19]/ Menu Title: #2 QA			Objective: [#]
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
All 5 assessment question slides should have the same layout and formatting. Background image: Office space takes up the entire slide The question number text appears larger than the multiple choice answer options, which are displayed below the question. All text has a transparent background; white text	[Slide Title] **Question #2** [Question] Following an incident, you should not use the affected systems until which personnel tells you to do so? [Answer Choices] 1. The software security system 2. The hacker 3. **The X CSIRC, your ISO, or your manager**	Select the best answer choice and click the submit when you are finished. Following an incident, you should not use the affected systems until which personnel tells you to do so?	Score by question with 1 attempt for each quiz question as the learner progresses through the quiz. They will be able to Retake the entire quiz at the end if they do not pass. Results slide 1.23; graded quiz slide – multiple choice. When learner clicks Submit, submit multiple choice and advance to next slide. The learner should not get *immediate* feedback with Correct or Incorrect feedback layers. They should answer all of the questions sequentially FIRST in the graded assessment, then receive their score on the Results page.

			If they do not pass, they can come back and review the quiz.

Notes:

Visual / Display:	Slide Text:	Narration / Voiceover:	Animation / Interaction:
All 5 assessment question slides should have the same layout and formatting. Background image: Office space takes up the entire slide The question number text appears larger than the multiple choice	[Slide Title] **Question #3** [Question] Select the four common types of security incidents. [Answer Choices]	Select the best answer choice and click the submit when you are finished. Select the **four** common types of security incidents.	Score by question with 1 attempt for each quiz question as the learner progresses through the quiz. They will be able to Retake the entire quiz at the end if they do not pass. Results slide 1.23; graded quiz slide – multiple choice.

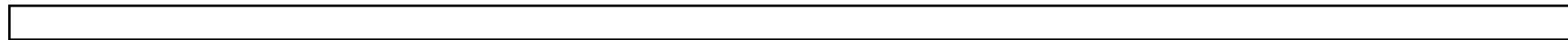|			
answer options, which are displayed below the question. All text has a transparent background; white text	1. **Accidentally sending a report containing confidential PII, SPII, and other CUI to a person not authorized to view the report, or sending it unencrypted.** 2. **Any security situation that could compromise X information or information systems (e.g., virus, phishing email, social engineering attack).** 3. **Allowing an unauthorized person to use your computer or credentials to access CUI.**		When learner clicks Submit, submit multiple choice and advance to next slide. The learner should not get *immediate* feedback with Correct or Incorrect feedback layers. They should answer all of the questions sequentially FIRST in the graded assessment, then receive their score on the Results page. If they do not pass, they can come back and review the quiz.

	4. **Loss, damage, or theft, of equipment, media, or documents containing PII, SPII, and other CUI.** 5. Using the "forgot password" link on a secure site.		
Notes:			

Slide [1.21]/ Menu Title: #4 QA			Objective: [#]
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
All 5 assessment question slides should have the same layout and formatting. Background image: Office space takes up the entire slide	[Slide Title] **Question #4** [Question] If anything suspicious occurs, you should document what you experience. Immediately write down any	Select the best answer choice and click the submit when you are finished. If anything suspicious occurs, you should document what you experience. Immediately write down any information that may be helpful to investigators.	Score by question with 1 attempt for each quiz question as the learner progresses through the quiz. They will be able to Retake the entire quiz at the end if they do not pass.

The question number text appears larger than the multiple choice answer options, which are displayed below the question. All text has a transparent background; white text	information that may be helpful to investigators. [Answer Choices] 1. **True** 2. False		Results slide 1.23; graded quiz slide – multiple choice. When learner clicks Submit, submit multiple choice and advance to next slide. The learner should not get *immediate* feedback with Correct or Incorrect feedback layers. They should answer all of the questions sequentially FIRST in the graded assessment, then receive their score on the Results page. If they do not pass, they can come back and review the quiz.
Notes:			

Slide []/ Menu Title:			Objective: [#]
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
All 5 assessment question slides should have the same layout and formatting. Background image: Office space takes up the entire slide The question number text appears larger than the multiple choice answer options, which are displayed below the question. All text has a transparent background; white text	[Slide Title] **Question #5** [Question] Drag the items into the boxes on the right to match their descriptions. [Answer Choices] ● You suspect that computer security, confidential information, or PII incident has occurred or is occurring. **[Stop Everything]** ● Call us if you suspect you have experienced a security breach	Select the best answer choice and click the submit when you are finished. Drag the items into the boxes on the right to match their descriptions.	This slide is a drag-and-drop interaction. There will be 4 phrases as drag items that the learner will need to sort between the four drop targets matching their descrptions. They will be set in rectangles of one of the palette colors. The drag items should appear in a scrambled order so they are not already sorted by type of privacy. Score by question with 1 attempt for each quiz question as the learner progresses through the quiz. They will be able to Retake the entire quiz at the end if they do not pass.

	or incident. Write down any information that may be helpful to investigators. **[The X Call Center]** ● Follow X policy and send an email to the same recipients of the original breached email or data spill. **[Send Mitigating Email]** ● Your manager and ISO are to review any and all incidents, and will check open tickets and reports provided by the X CSIRC. **[Incident Recovery Follow-Up]**		Results slide 1.23; graded quiz slide – multiple choice. When learner clicks Submit, submit multiple choice and advance to next slide. The learner should not get *immediate* feedback with Correct or Incorrect feedback layers. They should answer all of the questions sequentially FIRST in the graded assessment, then receive their score on the Results page. If they do not pass, they can come back and review the quiz.

Notes:

Slide [1.23]/ Menu Title: Quiz Results			Objective: [#]
Visual / Display:	Slide Text:	Narration / Voiceover:	Animation / Interaction:
Same format as Assessment Slide (1.17) Background image: Photo of office space on right half of the slide; text appear the left side of the screen.	[Slide Title] **Results** Your Score: **XX**% Passing Score: **YY**%	*[Narration only on layers]*	Use a Result side to show Success layer 1.23a when timeline starts if results are equal to or greater than the passing score. Show Failure layer 1.23b when timeline starts if results are less than passing score. Base layer will be visible (show through) from Success or Failure slide layers. Results variable reference shows the percent score only. Do not show the points variable reference.

| | | | Built in graded quiz variable reference displays learner score where **XX** appears on slide

80% to pass shown where **YY** appears on slide |
| --- | --- | --- | --- |

Notes:

Green diamond with slide text	[Slide Title]	[Narrator]	Review button: shows incorrect response when reviewing
	Quiz results	Thank you for taking the quiz. Congratulations! You passed. You can review your results by clicking on the review quiz button. If you are satisfied with your results and ready to move on, please click on the next button.	
	Good job! You passed the course.		
	Your Score: **XX**%		Next button: jumps to Slide 1.24
	Passing Score: **YY**%		
	[button]		
	Retry		
	Review		
	Print		

Notes:

Red diamond with slide text	[Slide Title] **Quiz results** Sorry, you did not pass this course. Your Score: **XX**% Passing Score: **YY**% [button] **Retry** **Review** **Print**	[Narrator] Thank you for taking the quiz. Unfortunately, you did not pass. You can review your results by clicking on the review quiz button. When you are ready to try again, please click on the retake quiz button.	Retake button: resets results slide and jumps to Slide 1.17 Review button: shows incorrect response when reviewing Next button: jumps to Slide 1.24
Notes:			

Slide [1.24]/ Menu Title: Congratulations			Objective: [#]
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
This slide has a similar design as the Welcome slide. Background image:	[Slide Title] **Congratulations!**	Congratulations on completing the Introducing Incident Response & Reporting course. Now you have the knowledge you need to ensure that if you	Directions badge glides in using motion path at the top right of slide

Photographic image of persons hand holding a cell phone to open an security application Center of photo has a white background for text	You have successfully completed Introducing Incident Response & Reporting [Direction] Click on the close button to exit the course. [button] Close	were to experience a security incident you will know what to do immediately and who to contact to protect their personal information. It requires a little extra effort, but you and your customers will be happy with the results. You may click the close button to exit the course.	Background image: Photographic image of a lock being open or visual to indicate success.

Notes: