Introduction

Table of Contents

Cyber Infrastructure Survey (CIS) Training Course

September 2017

Homeland Security

**001 Instructor: All right. Welcome to the Cyber Infrastructure Survey Training class. This is the first offering.

Copyright 2017 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM17-0615

**002 Copyright and distribution statement.

About the Course

This course prepares both new and experienced Cybersecurity Advisors (CSAs) to perform a cybersecurity assessment of a critical service using the Cyber Infrastructure Survey (CIS).

**003 So what the course is intended to do. As I was saying earlier, it's really meant to introduce everyone to the CIS, and it's structured for both entry-level people that may or may not be CSAs, as well as CSAs, and it's geared at trying to solicit accurate answers to the CIS, while you're in the process of performing one.

Attendee Introductions

Going around the room, please tell us your

- name,
- organization,
- position,
- reasons for attending this course, and
- expectations for the course.

**005 So what I'd like to do, I know that everyone here is from DHS, but I would still like to do introductions. If you could just give us your name and what your expectations are for the course. Right.

I am Phil Scolieri from CERT. I'm hoping that this meets your expectations and actually prepares you to actually solicit the accurate answers in the CIS itself.

Instructor 2: My name's Gavin Jurecko. I work with Phil. I'm going to be assisting in delivering the content today.

Course Objectives

After completing this course, you will be able to

- perform a cybersecurity assessment using the CIS,
- develop a basic understanding of the CIS,
- set up a CIS assessment on the portal,
- describe the CIS domains,
- use the CIS dashboard to present results to the customer,
- understand the intent of the questions, and
- manage the CIS interview process to elicit more accurate and complete answers.

**006 So Course Objectives. After the, completing the course, you know, you will be able to perform an assessment. Some of you, as you've said, are already doing that. Some are not. Some are brand-new, so this will apply to everybody.

Develop a basic understanding. You should be able to describe the domains. Also understand the intent of some of the question and question types, right, and relationships between the domains themselves and how to manage the interview process and actually elicit more accurate answers.

Course Outline –1

IP Gateway Portal
- demonstrates logging into the portal and how to add and edit a CIS, and explains the CIS workflow in the IP Gateway

Introduction to the CIS
- explains the CIS and its benefits, and introduces the dashboard and the decision analysis methodology

Identifying a Critical Services
- explains how to identify critical services and scope these services for the CIS

Administering the CIS
- introduces the types of questions, how to answer questions effectively, and the CIS domains

Homeland Security

**007 Course Outline. There's a beginning module on the IP Gateway portal. Some of you've been working with it. Some have not. So this'll be a good entry point for some of the people here.

Introduction to the CIS. We're basically trying to explain the benefits and introduce the dashboard and what's behind the dashboard.

Identifying a critical service. So there's a separate section on that, right, and how that applies to the

Administrating the CIS. We'll kind of review the question types and how those should be answered.

Course Outline –2

Managing the Engagement

- explains the process followed in managing a CIS engagement and discusses the use of the CIS dashboard

Question Intent

- provides information for each domain, including concepts and terminology, training tips and clarifications, quality assurance aspects, and best practices

**008 And there's two more sections. There's an overall section on Managing the Engagement that's basically going to walk through what that day and any preparation for that day looks like and what the expectations are, and Question Intent. So this is where we will go through each domain. We will be including training tips that we saw when it was being administered. Also clarification, some of the quality assurance aspects that come up, as well as mention best practices that the CIS tries to get to that are more organizational, where you would be able to voice those to an organization, like, "What is a best practice in this area?"

Logging into the IP Gateway Portal

Table of Contents

IP Gateway Portal

September 2017

**001 Instructor: All right. So the next area that we're going to discuss is the IP Gateway Portal. We're going to start at the beginning, how to login, go through how to add assessment.

**002 [Notice]

IP Gateway Portal: Objectives

After completing this section, you will understand

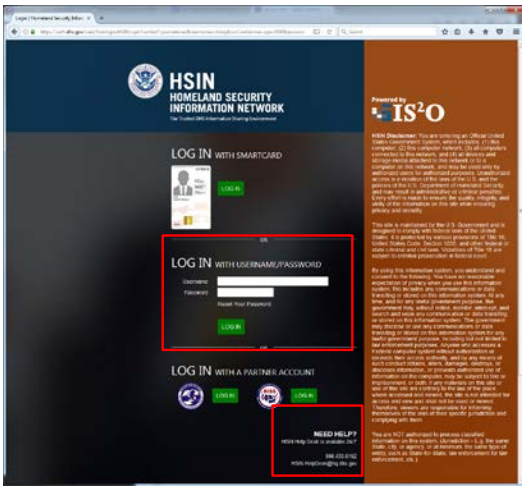
- how to login to the portal,
- how to add and edit a CIS, and
- the CIS workflow.

**004 So the objectives of this section are how to login to the portal, how to add and edit a CIS, and also the CIS work through, workflow, within the IP Gateway portal.

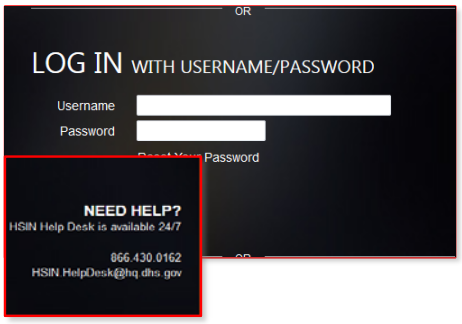
Login Page

Login Page

https://ipgateway.dhs.gov



- Ways to Log In
  - Username/password
- Help



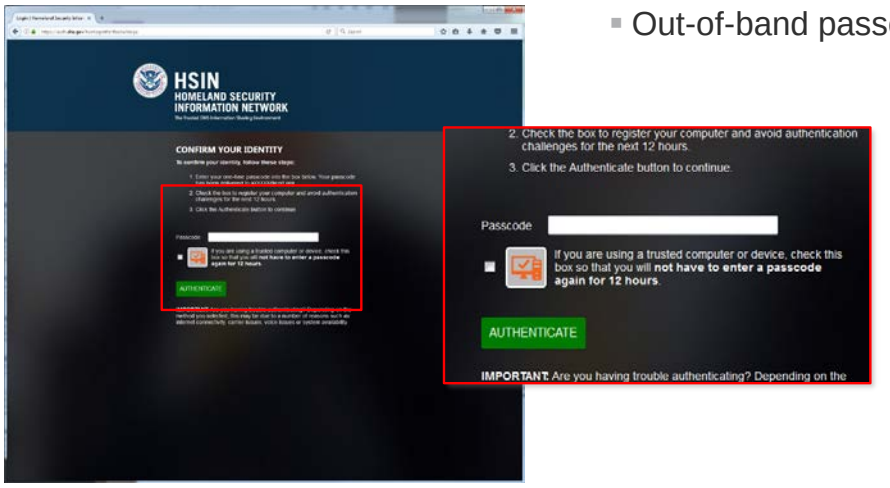
HSIN is leveraged for Single Sign On to the IP Gateway Portal.

Homeland Security

7

**007 Okay. So to get to the actual IP Gateway, you want to use the link ipgateway.dhs.gov. Once you go to that site you'll be presented with a similar screen. We're going to want to focus in on the login using a username and password.
There's also a Help section down at the bottom here. If you need help, you can either call the number or submit a ticket to the Helpdesk to get help from the IP Gateway Portal Helpdesk.

Passcode



- Out-of-band passcode

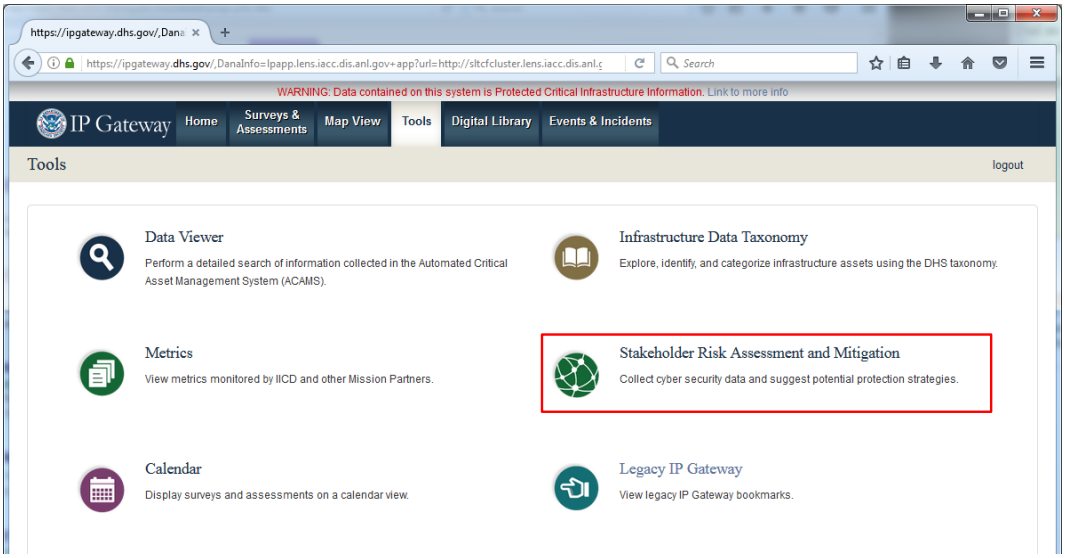
**008 After you enter your username and login, you're going to be required to get a out-of-band passcode. There's a couple different ways you can get this passcode, either via voicemail to your cell phone, a text message to your cell phone, and also you can get an e-mail with a code. Once you receive that code, it's pretty seamless. It happens pretty quickly. Enter it in to the passcode box and click Authenticate.

Getting to the CIS Portal –1

Homeland Security

**009 And then you'll be taken to a screen that looks like this. For the purposes of this training, we're going to focus on this Tools tab. So click on the Tools tab.

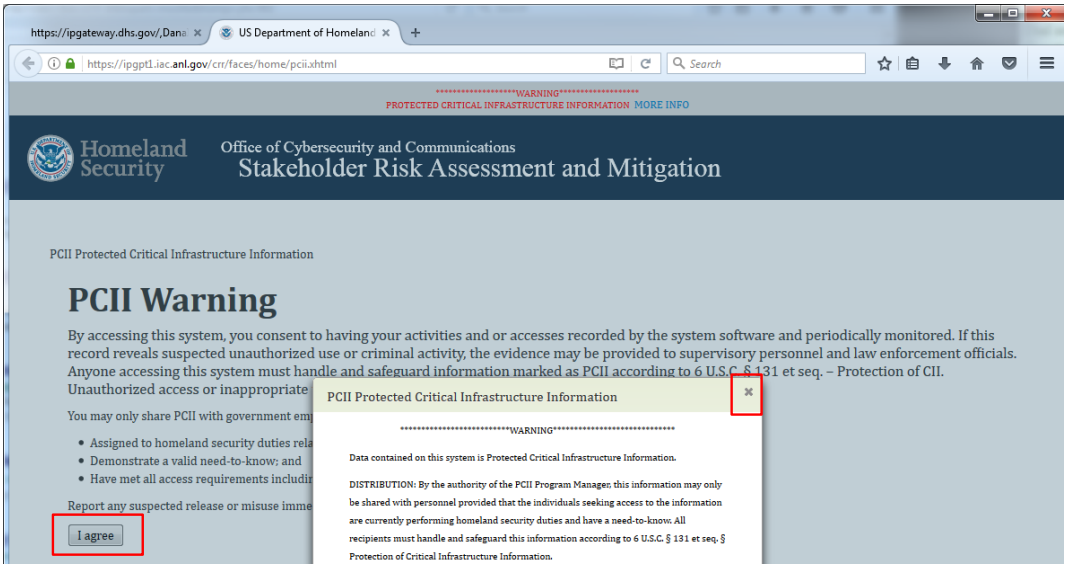
Getting to the CIS Portal –2



Homeland Security

**010 And then you will be presented with this screen. The CIS and all of the assessments live in stakeholder risk assessment and mitigation, so click on that whenever you get here.

PCII Warning



Homeland Security

[DISTRIBUTION STATEMENT F] Further dissemination only as directed by Department of Homeland Security (DHS) Office of Cybersecurity and Communications (determination date: 2017-09-05).

11

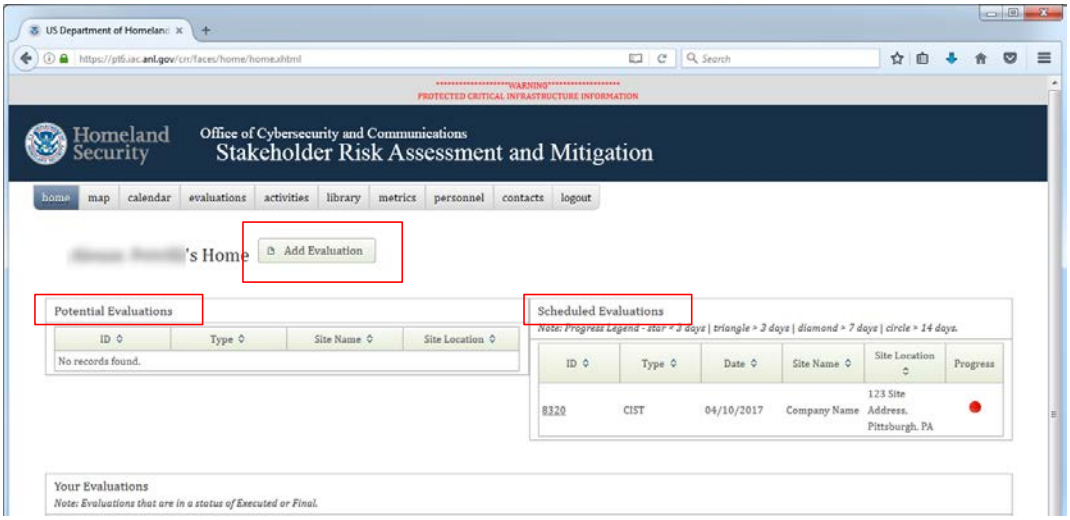
**011 And you'll be taken to this screen. So this pops up every time. It's just a PCII warning notating to the user that any time you go in here you will be viewing PCII information. Click on 'I Agree'.

The Workflow

Table of Contents

HomePage

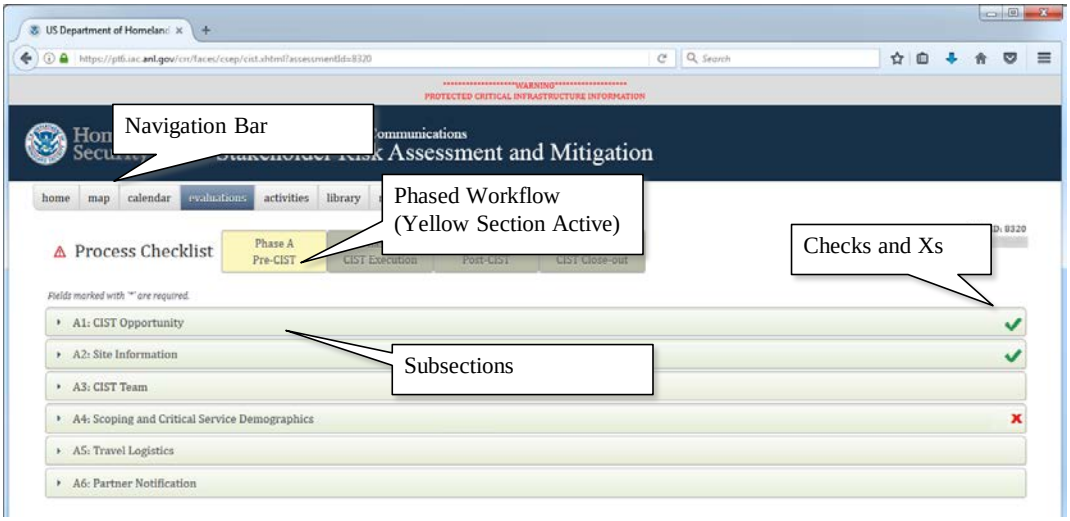
Add and Edit



**013 So what you see here is the homepage for anyone's portal, so you can add evaluations. It has your potential evaluations and also your scheduled evaluations. So for each specific user, you know, if something hasn't been scheduled yet it's going to show up over in your potential evaluations. If you have it scheduled it's going to be over to the right, and if you want to add anything you click on Add Evaluation.

Process Checklist –1

Workflow and Layout Overview



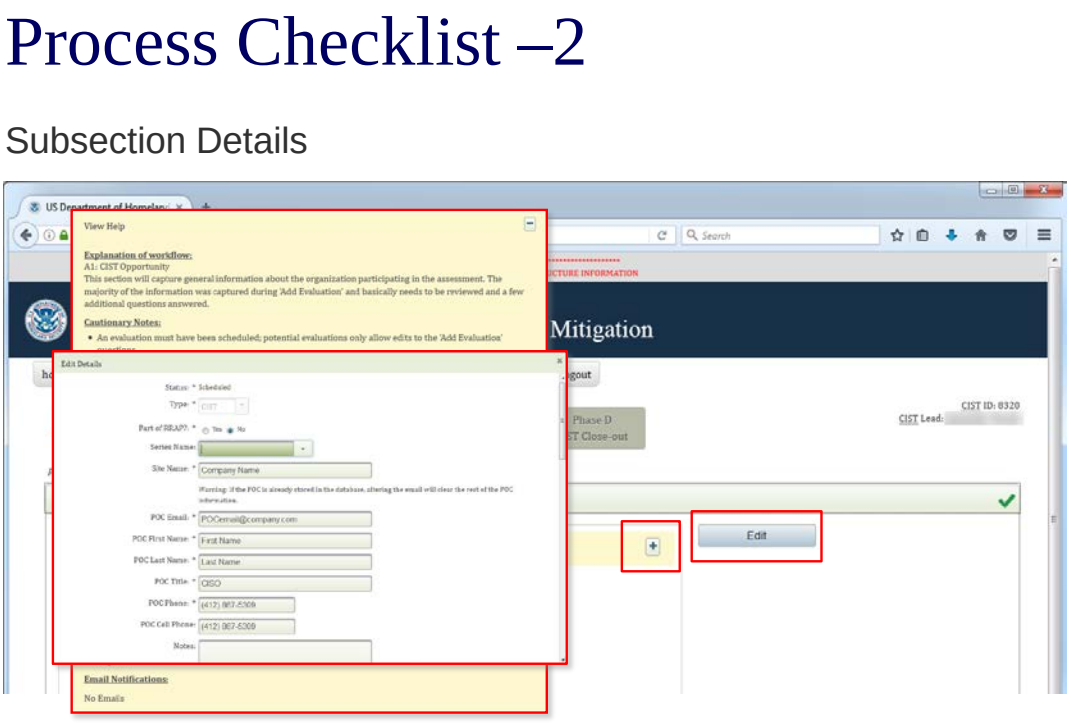
Homeland Security

14

**014 You can also see all the other evaluations that are scheduled, potential, whatever status that are at them by using this Navigation Bar and clicking on Evaluations. You can filter by all the different assessment types then, but once you're in an actual assessment there's distinct phases that you have to work through to get through a CIS and to get the different phases to actually access the survey to prepare the dashboard. So this bar across the top here has the different phases of the CIS process. When it's highlighted in yellow, that notates what phase you're actually in and each phase has a number of different subsections.

Some of these subsections are mandatory, others are not, but you have to complete a certain amount of them to actually open up Phase B and follow on Phase C of the assessment. You can tell the status of each subsection by the check or the red X to the right. If you haven't actually entered that subsection yet, I don't think there's a status that's shown up, but as soon as you kind of add something and you don't complete it, it'll present an X to you saying there's still stuff you need to complete in this section.

Process Checklist –2



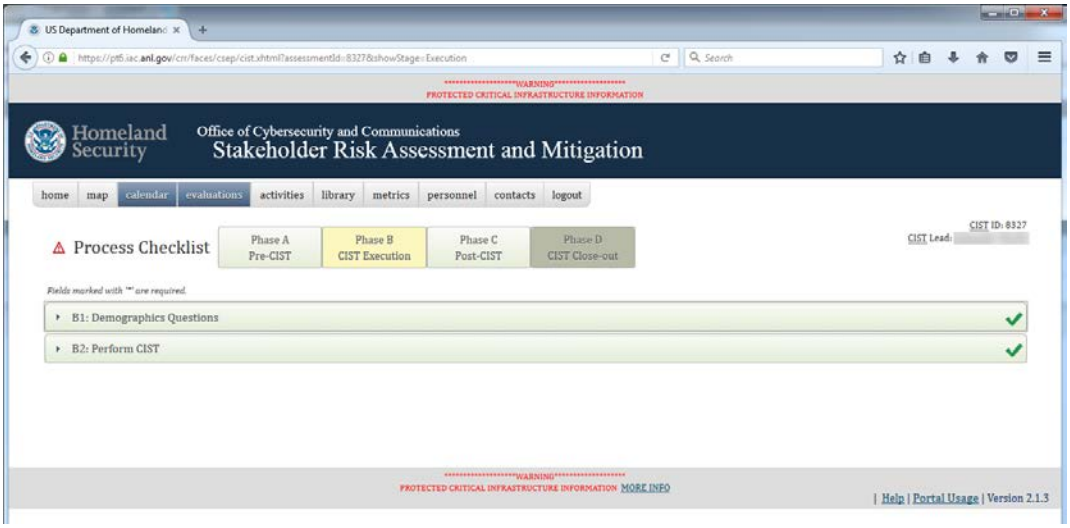
**015 All of the subsections can be expanded using this drop-down. You

can see here for the CIS Opportunity, you can see some of the point of contact information. Each subsection has Help text if you click on this plus sign here. It'll pop up some Help text and it tells you what's required, optional fields, different triggers to move through the workflow, so you really, the less familiar you are, these Help texts help you navigate through the different phases.

To edit any of the information in those particular subsections, there's normally some buttons over here that show up, so for this one, the Edit button, if you click Edit, you can start to enter information about the CIS. So site name. Also there's stars that indicate what's mandatory and what's not mandatory.

Process Checklist –3

Phase B

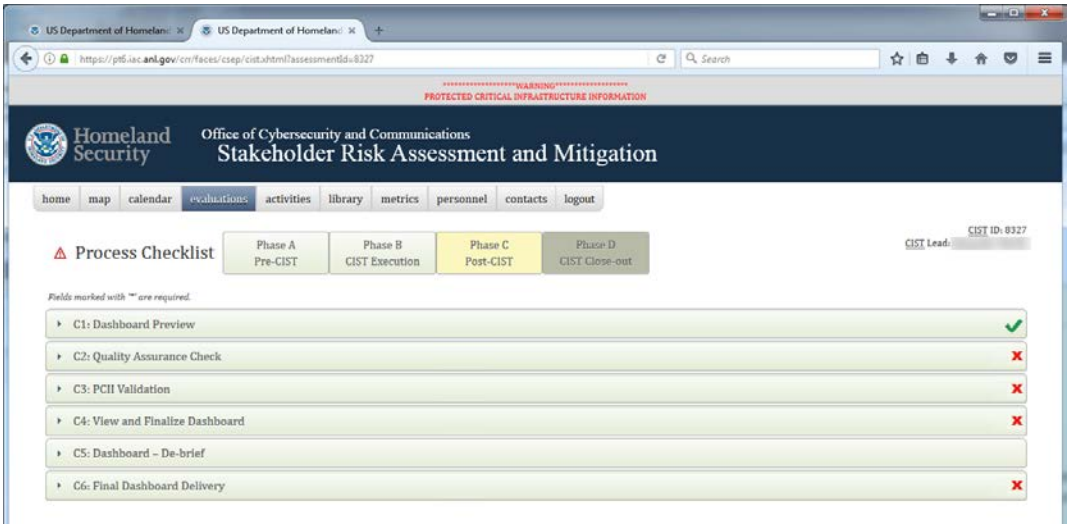


Homeland Security

**016 So now we're showing a graphic of Phase B of the CIS, so once you complete the required steps of Phase A it's going to take you and open up Phase B. You're going to be answering the demographic questions and then in Phase B too is where you can actually access the CIS survey. Once all the answers are submitted and you've actually completed the survey--

Process Checklist –4

Phase C

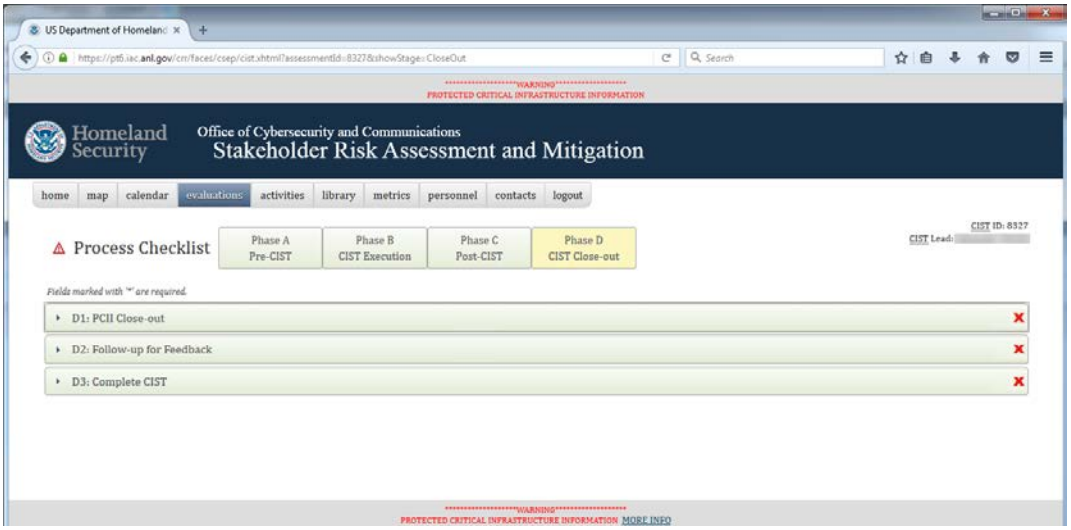


Homeland Security

**017 Phase C is going to open up. Here are the different subsections. We're going to go into a lot of detail on these later on.

Process Checklist –5

Phase D



Homeland Security

**018 And then Phase D is the CIS close-out, where you complete the CIS and get it archived in the portal as the complete status.

IP Gateway Portal: Objectives Summary

In this section, you learned

- how to login to the portal,
- how to add and edit a CIS, and
- more about the CIS workflow.

**019 So in summary, for this portal we learned how to login to the Gateway, how to add and edit a CIS, and we learned more about the CIS workflow, and that concludes this module.

Introduction

Table of Contents

Introduction to the CIS

September 2017

Homeland Security

**001 Instructor: So let's introduce the CIS.

**002 [Notice]

Introduction to the CIS: Objectives

After completing this section, you will understand

- what the CIS is,
- the benefits of using the CIS,
- the structure of the CIS,
- what the CIS is not, and
- the dashboard and the decision analysis methodology.

**004 So the objectives here, right. To get an understanding of what it is, what it's not. The structure, what the benefits are, and to get a basic understanding of the dashboard.

Introduction to the CIS: Topics

The CIS

CIS Dashboard and Decision Analysis

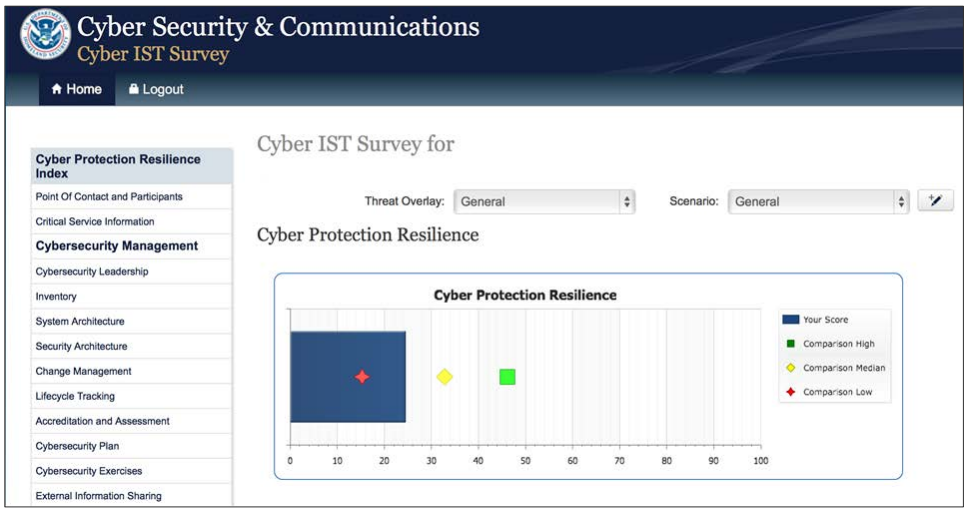
**005 So this is broken up into two subsections, if you will. The CIS and then the CIS Dashboard and Decision Analysis. Decision analysis is the methodology that is behind the dashboard. And we'll get into that further in the module.

The CIS

Table of Contents

What Is the CIS? –1

The CIS is the Cyber Infrastructure Survey.



Homeland Security

**007 So what does the CIS look like? Many of you are familiar with this. Some are not. This is a basic screen so you know what it looks like. You have items along the left side. What you're seeing is part of the actual dashboard here that is delivered to the customer at the end of the process. Okay? So it's just to familiarize yourself and give you some conceptual view of what the CIS looks like in the system.

What Is the CIS? –2

The CIS is

- a structured, interview-based assessment of the cybersecurity practices an organization uses to support its critical services (CSs),
- a survey that is focused on cybersecurity controls grouped under five domains, and
- an effective, repeatable technique used to assess a CS.

Key Fact

The information gathered during a CIS is protected under the Protected Critical Infrastructure Information (PCII) Program.

Homeland Security

8

**008 So what is the CIS? It is a structured interview process, right? It is around a critical service. Right. Not multiple. A single critical service, okay? A survey that is focused on cybersecurity controls. So this is where it differs for some of the other assessments. This is very much control-based. All right. It is, however, an effective repeatable technique, right? So it is something that can be done over and over again by multiple people. You should be able to solicit accurate and consistent answers between different people that are performing a CIS.

So a key fact, which many of you know, the information is protected under the PCII program.

The CIS at a Glance

The CIS at a Glance

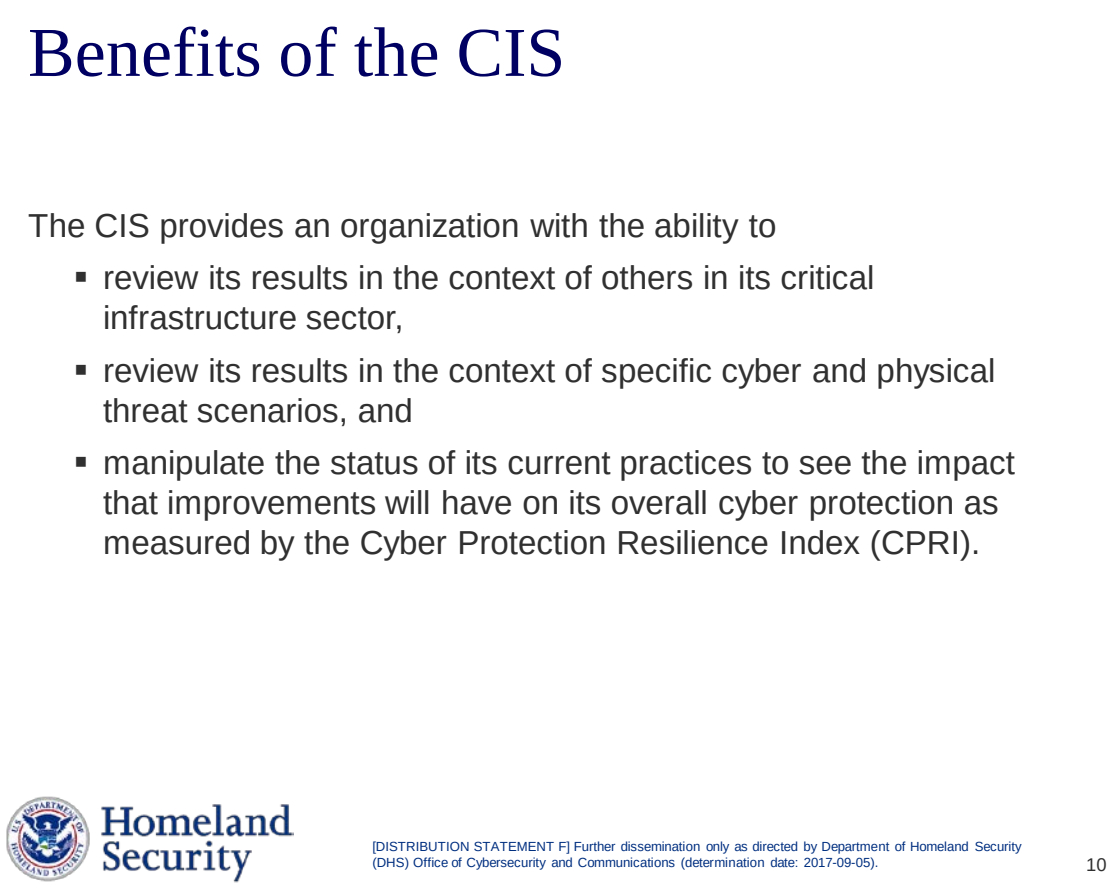
Purpose: To calculate a comparative analysis and valuation of the protective cybersecurity measures that are in place	The CIS is a survey instrument that is useful in limited situations, such as in new and potential partner organizations, as a relationship starter (e.g., an introduction to DHS critical cyber infrastructure protection) or with existing partners as a light-weight evaluation activity (i.e., no formal report and no formal recommendations).
Scope: One critical service (CS)	The CS is the focus and reference point for all questions, and is usually a key business system (such as an Electronic Medical Records System) or a process control system (such as a water filtration control network and SCADA system).
Time Required: 2½ to 4 hours	At 2½ hours, the interviews do not feel rushed, but 2½ hours does not allow for extended discussions.
Domains Discussed: The cyber-protective measures currently in place in the five domains	• Cybersecurity Management • Cybersecurity Forces (aka Personnel) • Cybersecurity Controls • Incident Response • Dependencies
Pre-Visit Preparation: Gather background information	Extensive planning is not necessary, but a pre-conversation can be useful to gauge and confirm interest, select the CS, and gather demographic data.
Interviewees: CISOs, IT security managers, and/or SMEs	The assessment works best when there are a limited number (1-2) of interviewees. If additional information is needed, the Cyber POC should be allowed to collect it. Typical SMEs include IT or service continuity planners, incident responders, vulnerability analysts, and network and system security administrators.

Homeland Security

**009 So the CIS at a glance. You're really calculating a comparative analysis and a valuation of those cybersecurity measures that are in place. The scope, again, is one critical service. Typical time frame is two and a half to four hours, right. That's what the expected time frame is. You guys may see varying amounts of that but typically I've been told that pretty much fits what an average CIS goes.

There are five domains within the CIS, right. They're listed here. We'll get into those further. Pre-visit preparation. The idea is you should not need a lot of extensive planning for this tool. However, you are expected to have some pre-assessment calls to define the critical service and other aspects. Point of contacts and so forth. Right.

Interviewees. There's a typical list here. You know, IT security managers, SMEs. Right. You typically will have one or two people most times. Could have more but that is typically what's expected.

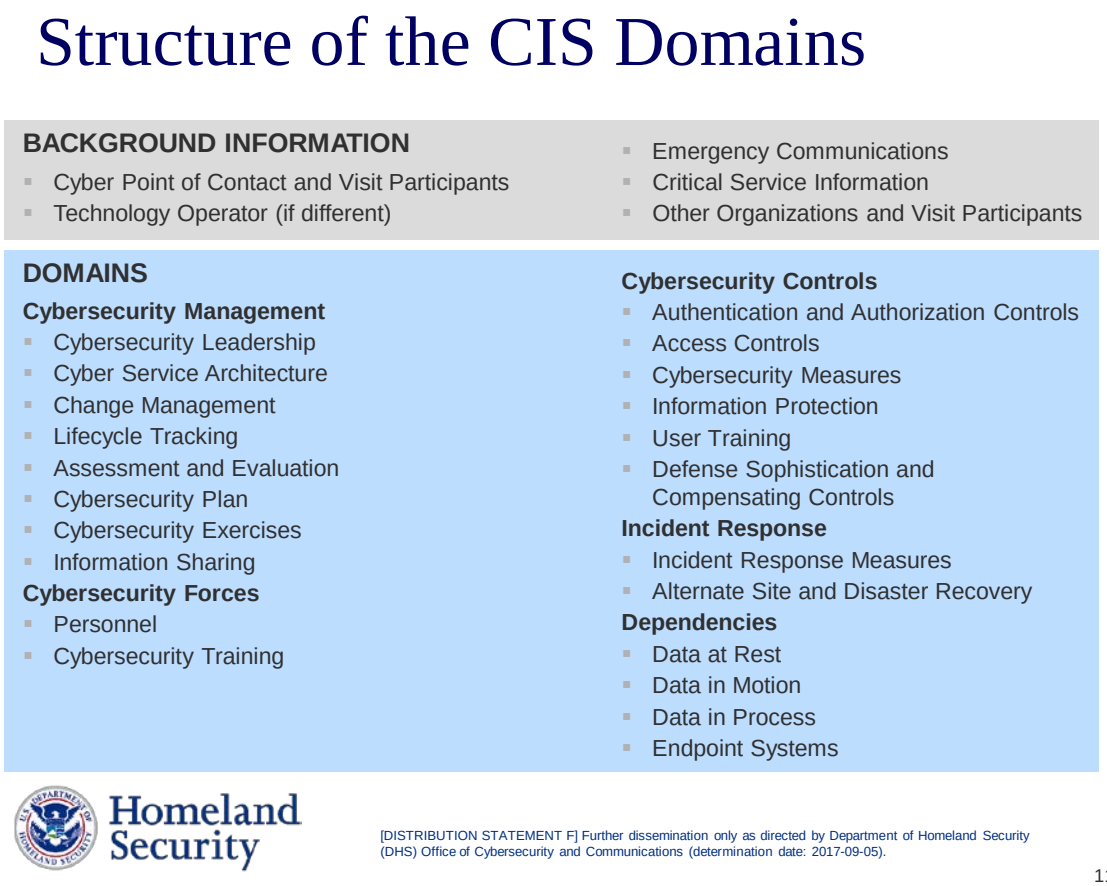


**010 So what are the benefits? Right. Provides an organization the ability to review their results in the context of other similar organizations. Right. So the demographics that's collected as part of the CIS helps accomplish that, and you'll see more of that later in some of the other modules.

Review the results in the context of specific cyber and physical threat scenarios, right. So the CIS has built into it four different threat scenarios and we'll discuss that in a separate module as well. If those scenarios are selected it will alter the index based on what controls are

considered effective against those scenarios, right, and to be able to manipulate the status of all the current practices to see what the impact is. So even as you're filling out the CIS with the customer, you'll be able to see the index score build, and you could also do this after the fact in some of the scenario capabilities that the CIS has. Again, so that'll be discussed in more detail in a different section.

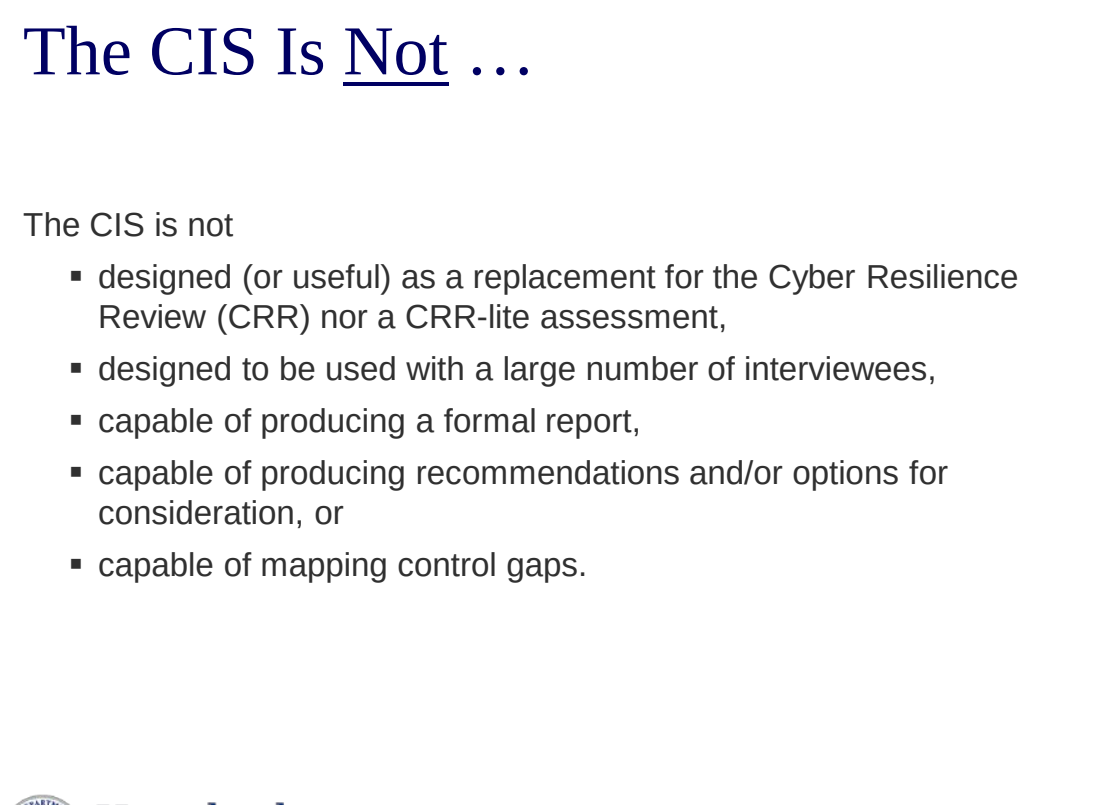
Structure of the CIS Domains



**011 What's the CIS structure look like, right? So there's six domains. We have five in blue and the background is in gray, right? The

meat of the CIS is really the five domains in blue. That's where you're going to be asking about all the various controls for those topics. The background information is important. You're going to be going over points of contact, trying to define a critical service, right. For example, right. So we'll be referring this, to this slide once in a while, just to refresh what the CIS looks like.

The CIS Is Not...



**012 What the CIS is not. Right. It is not designed as a replacement for the Cyber Resilience Review. It's not a CRR-lite. CRR's a different tool. It's looking more at process, right.

Overall process around practices. It's not asking as many discrete control questions. Do you have control X in place? Doesn't do that. It's designed to be used with a large number. It's not designed to be used, I'm sorry, with a large number of interviewees, right. It's also not capable of producing a formal report. So you don't have a report like you do at the CRR, right, to provide a customer. What the customer gets at the end of the process is the dashboard to review the results.

It's not capable of producing recommendations or options for consideration. That's not part of the CIS structure, and it's not capable therefore of mapping control gaps, right. So CIS is very targeted at trying to understand the controls and what benefits those controls bring to an organization.

IP Gateway Portal

The CIS is initiated and completed in the IP Gateway Portal.

Homeland Security

**013 Student: So it tells them that they have gaps but it doesn't tell them where those gaps are?

The CIS Is Not…

The CIS Is Not …

The CIS is not

- designed (or useful) as a replacement for the Cyber Resilience Review (CRR) nor a CRR-lite assessment,
- designed to be used with a large number of interviewees,
- capable of producing a formal report,
- capable of producing recommendations and/or options for consideration, or
- capable of mapping control gaps.

**012 Instructor: There's not enough information to say, you know, "Look at maybe a series and develop gaps across an organization," right. It does tell you if you go look at your results and actually look at how you answered things, you'll be able to see what controls that are in place and what are not, right, and you can experiment, with you as the end user, could then experiment with that or in a scenario planning and by changing answers to some things, and we'll get into this more, you'll see how the index moves up or down.

Student: Okay.

IP Gateway Portal

The CIS is initiated and completed in the IP Gateway Portal.

Homeland Security

**013 Instructor: So this is just a reminder that the CIS is initiated and completed in IP Gateway Portal.
Right. That's where it's expected to be done.

CIS Dashboard and Decision Analysis

Table of Contents

**014 So let's get into the CIS Dashboard and Decision Analysis.

CIS Dashboard

Cyber Protection Resilience

- The CIS dashboard displays the **Cyber Protection Resilience Index (CPRI)**.
- The goal of the CIS is to calculate the value of the cybersecurity measures that are in place.
- This value is referred to as the CPRI.
- The organization's CPRI is **dynamically displayed** on the CIS.

Homeland Security

15

**015 So this is the dashboard. This is what it looks like. So again, note that, you know, the dashboard displays the Cyber Protection Resilience Index. That's what's calculated as you answer questions about the specific controls. Right. The dashboard when delivered also provides comparisons to similar organizations, right, and your score, as you see here, is in the solid blue, and the high, median and low comparison points, right. So you can see how you map to the group of organizations that are similar to you. It's not the overall aggregate of organizations.

Right. We refer to the value as the CPRI for short, and this gets dynamically displayed not in this same way but as you are in a particular section of the CIS you will also see how that builds and how the answers you have affect the score and we'll get into more of that as we move on into some of the other sections.

Right. So the dashboard is really delivered at the end of the process. This is what we mean by that. When you're in the process, you're not really displaying the dashboard but a piece of it that will eventually become the dashboard.

What Is the CPRI?

The CPRI measures how

- the organization has invested in cybersecurity and
- controls contribute to an organization's CPRI (not equally).

The CPRI was developed using the **decision analysis methodology**.

As an organization successfully completes the CIS, dashboards are created that show

- the overall CPRI,
- the CPRI for each domain, and
- a comparison between the organization's CPRI and that of all organizations that have participated in the CIS.

Homeland Security

**016 So what is the CPRI? Right. It measures how the organization has invested in cybersecurity, right, and how those controls contribute to the organization's CPRI. So it's very specific. It's that value that you're really measuring with the CIS, right. So the assessment is based on the CIS and this values particular to the

Right. As an organization successfully completes the CIS, the dashboards are created, right, and it shows you what we showed you on the screen previously. Right. You see a CPRI for each domain and an overall CPRI as well, right, as well as the comparisons to like organizations.

Decision Analysis Methodology

The decision analysis methodology

- is applied widely to real-world problems,
- reduces bias and subjectivity,
- provides a structured approach to complex problems, and
- is defensible and ensures consistency and reproducibility of results.

The decision analysis methodology applied to CIS results in

- controls that are not always equal,
- weighted values for each cybersecurity practice in the CIS, and
- different controls that provide different levels of protection.

Homeland Security

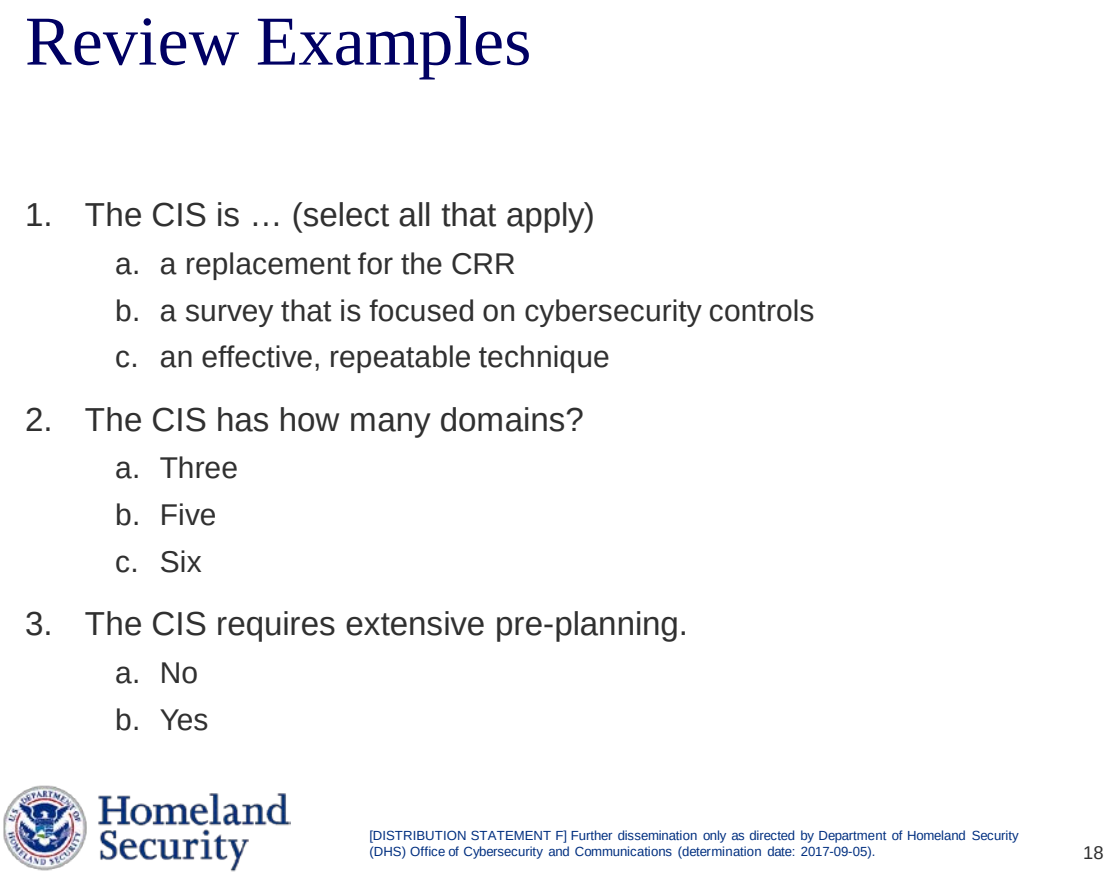
17

**017 So what's behind it? So decision analysis methodology. It's basically using a group of industry experts, if you will, from across different experts, and they're being pulled on what they believe the value of those controls are. So out of that, you get a series of weights that are applied to each control, and that's how that is really calculated. That's what's behind the dashboard, right. That's what's behind creating that and producing that CPRI index, right.

As you see here, it's a widely applied methodology. It provided a structured approach to build this and create the CPRI. Right. It's a

defensible method. Apply to the CIS. No. You have to understand that not all controls are equal. They do not all have equal weights. Right. So some are going to affect the score more than other. Right. Different controls then provide different levels of protection. Right. And that was all arrived at through this methodology that was put in place to create the

Review Examples



**018 So review. The CIS is... Select all that apply. Is it a replacement for the CRR?

Student: No.

Instructor: Right. What about is it a survey that is focused on cybersecurity controls?

Student: Yep.

Instructor: An effective, repeatable technique?

Student: Yep.

Instructor: The CIS has how many domains?

Student: Five.

Instructor: Right. So we should say, like, is it five? There's five core domains. How many total?

Student: Five.

Student: Yeah. We're taught five domains.

Instructor: Yeah. There's five core domains, right, and it's a little bit purposely like this. So there's six overall, but there are five core domains where the questions are asked. Right. So yes.

The CIS requires extensive pre-planning?

Student: No.

Instructor: No. And I--you guys can tell me. Is that what you experience in the field? It shouldn't need a lot of pre-planning, right?

Student: That's right.

Conclusion

This page intentionally left blank.

**020 So that concludes this section. We'll prepare for the next.

Introduction

Table of Contents

Identifying Critical Services

September 2017

Homeland Security

**001 Instructor: Okay. So we're going to pick it up with identifying a critical service. This is going to be a brief overview of, you know, what we consider a critical service and how it applies to the CIS. Right. So we've already shown in the previous sections that the CIS is geared to evaluate a single critical service.

[DISTRIBUTION STATEMENT F] Further dissemination only as directed by Department of Homeland Security (DHS) Office of Cybersecurity and Communications (determination date: 2017-09-05).

**002 [Notice]

Identifying Critical Services: Objectives

After completing this section, you will understand

- the critical service model and
- scoping the CS for the CIS.

Homeland Security

**004 So the objectives. As I stated, completing this section, you should understand the critical service model and also scoping the critical service for the CIS assessment.

Identifying Critical Services: Topics

Critical Services

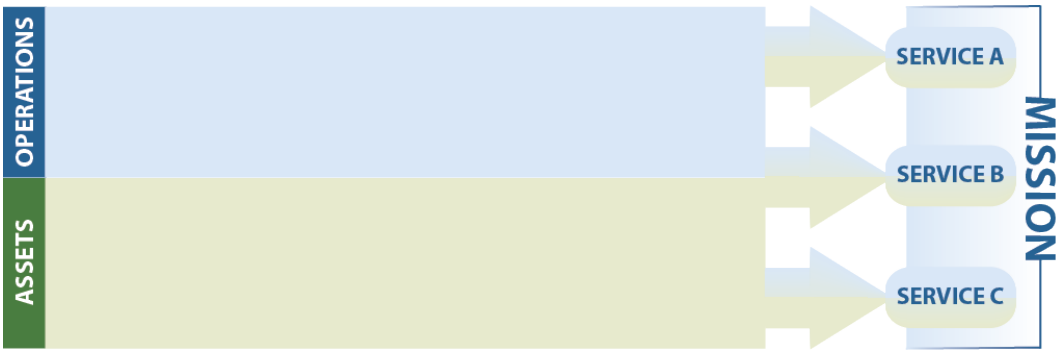
CIS Scoping

**005 First part is going to be critical services. You know, what are they? And the second part will be scoping.

Critical Services

Table of Contents

Identifying Critical Services



High-value services

- are critical to the success of the organization's mission;
- support the accomplishment of the organization's strategic objectives;
- must be identified, prioritized, and communicated; and
- are the focus of protection and sustainment activities.

Homeland Security

**007 So what we're showing here is the building. We're going to go through and build the model itself of what a critical service is. So as you notice, you can have one or more services that actually accomplish an organization's mission, right. Reason we tie it to a mission is that what we should be evaluating is a high-value service, right.

So as an example, in a water authority, we want to evaluate something like water purification, right, or water distribution, not necessarily the e-mail system. Right.

Student: So if you identify more than one critical service, can you--

Instructor: You want to narrow it down to one.

Student: Okay.

Instructor: Right. So in discussions, you will actually do that. They may mention three or four, and in your discussions with the customer you will narrow it down to what they think the most appropriate one is for the day.

Student: Okay.

Instructor: Right.

Student: Or they could come back and do the other three on separate dates.

Instructor: That's correct.

Student: Okay.

Instructor: And organizations have chosen to do that, right, and this is where they'll get into a series.

Student: Oh, got it.

Instructor: Either by choosing one, say, on an agency basis or within a single agency. They want a broader view, you may go back and look at three or four of them.

Student: Got it.

Instructor: Okay. Yes, sir?

Student: And is this the same process that's used for both the CRR and the EDM or is it different for the CIS than it is for the other two?

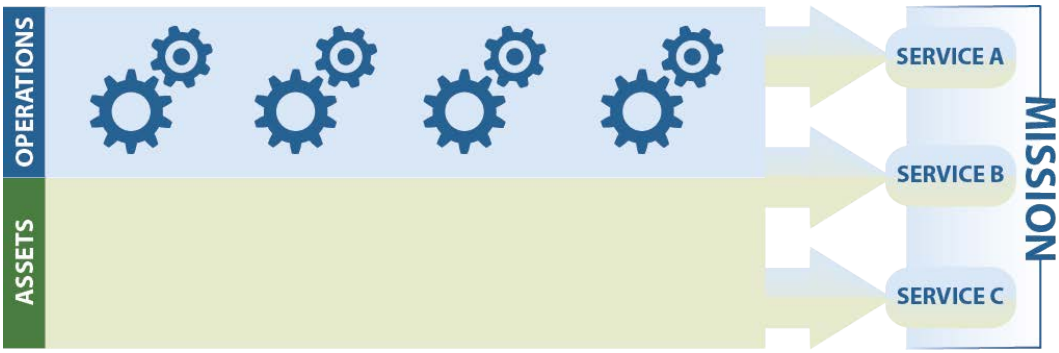
Instructor: It's the same.

Student: Yeah.

Instructor: Right. The difference is in the CIS you are actually going through as part of the CIS and defining and recording what the service is. Right. And that's done in that background section, as you guys that have done these already know. All right.

So high value services are critical to the success of the organization's mission, right. As we've been discussing. They should be supporting the organization's strategic objectives, right. They should be identified, prioritized and communicated, so typically there's going to be areas where a person within an organization actually can go look at and find what the critical services are if they don't know it.

Productive Activities and Business Processes



A service is made up of operations and assets that perform one or more productive activities.

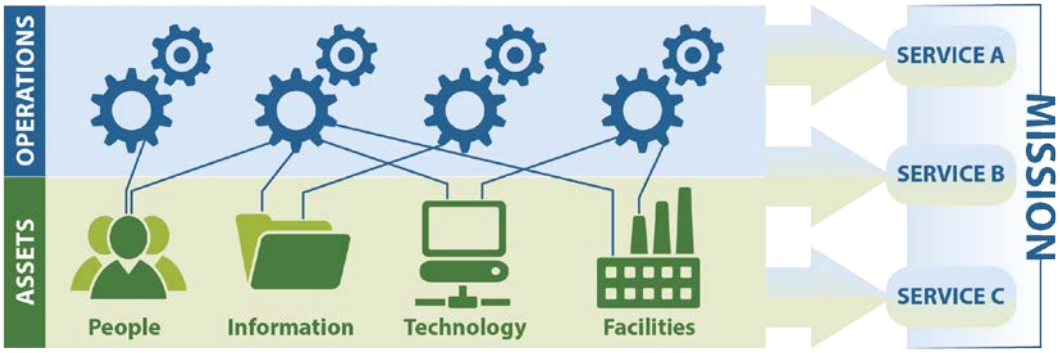
An organization uses its **assets** to perform **productive activities** to provide operational **services** and accomplish its **mission**.

Homeland Security

**008 So how this builds. You're going to have business processes, right, and operations that actually support that service. Right. So which may mean in that water authority you have an entire SCADA system to help support how the purification is done, right. And that may not be all of it. There might be other operations such as you need to transfer maybe regulatory data to different file servers or so forth at corporate, possibly, right, and know that becomes important because without that data it may affected the purification of water. Right.

So an organization also uses its assets to perform those productive activities, right.

Assets Support Services



**009 So that's what we're showing here. Now, typically, in the other assessments, we're looking at all assessments, really. We're looking at these four asset types, right. So as you can see in a diagram, a single asset may support multiple business operations and as you can see here from the color scheme, they may also support multiple services. Right. You may have some assets that do that. That's okay, right?

Your discussion will center around that single service. Right. So what are some of these assets? You know, people. It could be people that operate and monitor the service, right. Anybody important to delivering the service would be considered a people asset.

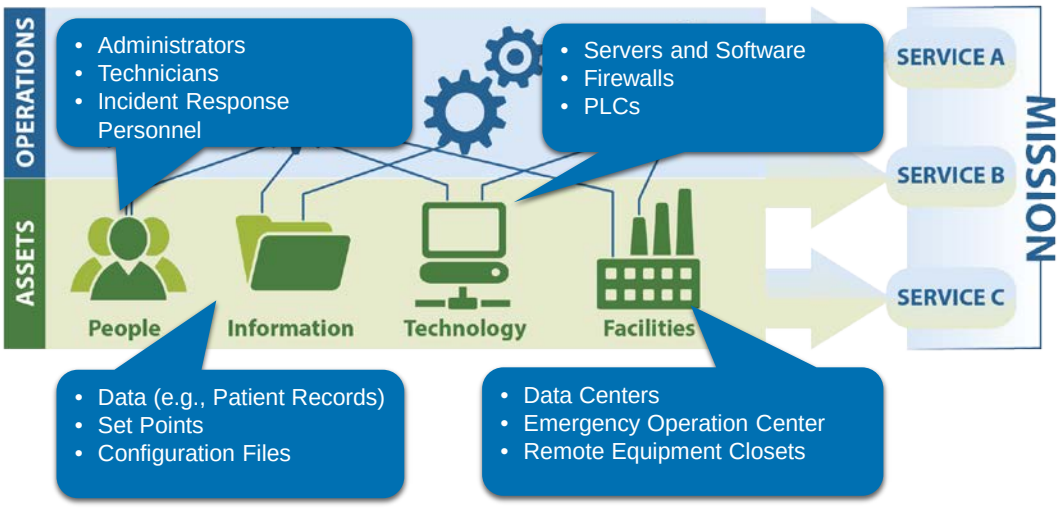
Information is just that. It's data associated with the service. Now, that can be anything from, say, that regulatory data that you produce, but it would also be configuration files that you need to reconstitute the service if there's an interruption, right. So maybe the network configuration files or the server configuration files. Things like that are considered information assets, right.

Technology. So notice in technology you're looking at system level assets and software level assets. That's really your technology layer. The software itself is not information. It's part of your technology layer. Right. So that SCADA system software may be important. The database software they use may be important, right. So as you're defining the high-level view of the service with the organization.

Now, facilities, where the services is performed, may include data center. It may include very important kind of regional hubs of technology, right. In a water authority you may have huts that are in the field that some may be more important than others, right. So that you'll have to kind of work through with the organization, right, before the assessment begins.

Now, a distinction to make here along with the CIS is it doesn't focus on facility assets as much as the other assessment does. It does do it in certain sections of the CIS, but not throughout.

Asset Examples



**010 So as examples, what we've overlaid on top here are examples of some of the asset types. Right. So as you can see, technology, servers, firewalls, PLCs. Whatever is important for the delivery of the service. If it's going to affect the delivery of the service, you want to consider it to a great degree. Right.

CIS Scoping

Table of Contents

CIS Scoping

Cyber Infrastructure Survey (CIS) Training Course

**011 Scoping.

CIS Scoping –1

As part of a CIS, you must define the CS and consider

- its connection to the critical infrastructure,
- whether it is strategically important to the organization,
- its significance to the organization's mission,
- whether it has an external focus (i.e., is of value to external stakeholders),
- whether the organization has identifiable ownership (i.e., authority) over assets that contribute to it,
- who provides inputs to it and who gets outputs from it,
- the assets that are used to support those providing inputs and getting outputs, and
- where these assets and people reside.

Tip

Set the scope to only what can be clearly defined based on the above criteria.

Homeland Security

**012 So we've kind of started to talk about that. As part of the CIS you must define the critical service, and by the way, we're using CS to, for critical service here. You'll see that throughout, and consider its connection to the critical infrastructure. Its significance to the organization's mission. You know, who provides inputs to it and who gets outputs from it. That may be important, right.

Users of the service. If they're expected to do certain functions and they cannot perform that function, then I would not consider the service as being delivered. Right. Where

the assets and people reside, that's where the facility aspects come in. Right.

Notice the tech tip here. Set the scope to only what can be clearly defined based on the criteria above, right. So you want to have a discussion around this water authority, say, "What are the major aspects along those assets we discussed to deliver the service of purification?" Right. So you may have a mix in that instance of PLCs and control systems, as well as maybe some important business systems to consider, and then how that information is delivered, right. So certain network aspects are going to be important, right, and it may not always be Ethernet, it may be radio or something else, right.

So though you just need to kind of get that good, high-level understanding in that discussion previous to the assessment, so everybody's aware of the assets that you will be discussing during the assessment. Because now you've scoped it and people will tend to drift on, "Well, over here we do this." Well, that's not part of the service. We need to answer for this critical service, okay?

CIS Scoping –2

To identify how an organization's operations support national security interests, services are sometimes aligned with descriptions of a critical infrastructure sector's functions.

This alignment makes it possible to identify assets that are important for achieving sector missions.

**013 Student: So, and guys, you can help me out with this one. So in going into a meeting to do the scoping, which is either on the phone or in person, right?

Student: Yeah.

Student: They may define five or six different services but they have to pick one for the particular assessment that we're doing at that particular time.

Instructor: Mm-hm.

Student: Right.

Student: Okay. So then my follow-up question on that would be, okay, you've picked this service. You also want to have assessments on these also in the future?

Student: That's usually something I would approach after. Let them see the value of the assessment first. One of the nice things about the CIS is that you can go back in and they can actually kind of use it to assess themselves afterwards using the dashboard, because, you know, your time is going to be very precious and important, so if you have time to go back in it's a good thing to do. But once they have the dashboard, there's a lot of this they can do themselves too, once they understand how the questions are being asked.

Student: Okay.

Student: So maximize your time with them. Come back in and discuss the dashboard with them afterwards, show them how they could use it for their other services, would be a better use of your time than trying to do a lot of these over and over again for the same customer.

Student: Got you.

Student: I found that getting the organization that you're talking to understand the concept of what a critical service is, that's usually foreign to them, and it's almost, sometimes I say it's a made up term, like EHS, that we use for the

purposes of the inspection or the assessment. Once they get their head wrapped around what you're actually trying to get them to categorize and drill down to, it usually goes pretty well from there.

Student: Yeah. Because I--you're right. Initial conversations they're looking at enterprise as opposed to critical service.

Student: You'll have people say e-mail. You'll have people say, "my web."

Student: Yeah. They'll try and go their core network and you have to try and get them away from, because a lot of the people you're going to talk to are going to be IT people, and they're going to be thinking in terms of systems and you want to say, "No. I need you to think about it as a business operation, a service line."

Instructor: Yes. Exactly.

Student: And all the systems that will be supporting that service line. So nuts to bolts, start to finish.

Instructor: Yeah.

Student: Everything that we're going to touch to get this widget produced or whatever it is or distribute whatever it is you're doing, you might be bringing in several different of your key systems. There might be an ICS system here, your core network might be part of this.

Instructor: Mm-hm.

Student: And then you're going to have, you know, a cloud service over here. All of that is part of your critical service but there are five or six systems that make up that critical service.

Instructor: Right.

Student: Once you approach it that way they're like, "Oh, I can put multiple systems in for this as well."

Instructor: Right.

Student: Yes.

Student: Ah.

Student: If your e-mail is really critical to it then you can pull your e-mail in but we usually try and stay away from the e-mail part.

Instructor: Right. So this has its basis in risk management, right. So what you'll see and what's the way we teach it is there isn't an organization that can afford to do all these things enterprise-wide. The intention is to focus on what's most critical in the organization. That's why we're focusing on that service, right. So if their mission is the purification of water or the distribution of that water, then that's what you're building the service around, one of those components. Doing multiple services at once muddies the data, because you're not going to--you might be doing something over here that you're not doing over here, so now everything

becomes incomplete, right, so--or you're really doing it, as you'll see in the CIS, you're going to be looking to define what that least common or least effective method is because you're looking for that weakest point.

We're going to get into some of that in a future training, right. So there's really a basis for this in risk management and you're trying to focus your resources on what's most important. Right. That's where this concept is actually helping them scope it as well, and Tony and I were just at a customer site where that became very apparent to the senior management and they're like, "We've been looking at services wrong. We should be looking at it more from that business component that would encompass all this. What's the business mission?" Okay?

Instructor: So we've kind of discussed this slide.

CIS Scoping –3

To understand the critical functions of each sector and manage the CS discussion, become familiar with critical infrastructure and key resource (CIKR) sector specific plans.

As an example, members of the healthcare and public health sector identified six private-sector functions in its sector-specific plan:

- direct patient care;
- health information technology;
- health plans and payers;
- mass fatality management services;
- medical materials; and
- laboratories, blood, and pharmaceuticals.

**014 I'm going to move on. Okay. So to understand the critical functions of each sector and manage the CR discussion, become familiar with the sector specific plans. In some of the sector specific plans, as you'll see in the example here for healthcare, at a sector level they're defining what they believe the critical service of the sector is, right. So this will help you start to think about the critical service for maybe the organization you're going to.

Not all of the sector specific plans have this information but some do, so it's worth becoming familiar with them. So in this example, we're

looking at healthcare in the slide. There's another example in the notes at the bottom of this, right, and it's interesting to see.

So direct patient care, right. That is really the service, so might, you might say patient care in the emergency room, and to Klint's point earlier, that'll pull in the, you know, the records management, the medical records system. It'll pull in the networking to deliver what the doctors need to be able to see, you know, the x-rays or whatever, right, so to deliver that service of patient care, you're going to have all these various components or systems and the assets that make them up. Now you've scoped it and it's not the entire enterprise. It becomes very specific.

Instructor: Yeah. If one of you guys asked me to support a scoping call, I'll check these out before the call just to kind of guide the conversation. It gives you a starting point at least whenever, you know, a lot of the times they come in very, very broad and it helps you as a guiding point to say, "Let's try and focus on some of these that the sector defines."

Student: Where can we find the large list of these, like, for every sector?

Student: So I normally will Google the sector and then the sector specific plan. I don't know the exact link. It's out on dhs.gov somewhere, I believe.

Instructor: Mm-hm.

Student: But normally if you type in the sector and then sector specific plan, that'll at least get you to one and you can kind of see what other ones are available there.

Instructor: I'm usually trying to find them, but you can--they're pretty easy to find, right. And DHS is actually, the sponsor's kind of the wrong word, but they're the main contact for some of these plans.

Student: Yeah. I think it might be infrastructure protection, I think, who might help.

Student: IPs.

Instructor: Yeah.

Student: IP. Right now it's SSP.

Instructor: Mm-hm.

Student: Have you run across instances where a particular company will be over through multiple critical infrastructures and trying to help them scope to the, you know, the one, you know? Like, let's say somebody's in the chemical sector but they're also in the water sector at the same time.

Instructor: Yeah.

Student: How do you help them scope, you know, using these? If they're saying, "Hey, both of these are really important to how we

operate," is there a rule of thumb like how to lean them toward one versus the other or is it just based on--

Instructor: What I would do is have the discussion of which one they feel is most important to do first based on their knowledge of the business, because I'm, being there a day, I'm not going to be familiar with their business, right, and try to help them arrive at that conclusion kind of on their own and at that point, like was mentioned earlier, I would recommend that maybe we come back and do the other one because it's also very important, right, and they can decide if they want to do that.

But you can't--doing more than one service will just muddy the data. It will be no benefit to them.

CIKR Sectors

**015 So a representation of what the sectors are. Most of you would know this. You know, new people would not necessarily know this, right. So there's 16. There used to be 18. That was trimmed down recently. This is what's remaining, and I do not have a feel for the CIS data to know if we're actually doing, you know, CIS assessments in all the sectors or if it's typically probably maybe half of them or three-quarters, right.

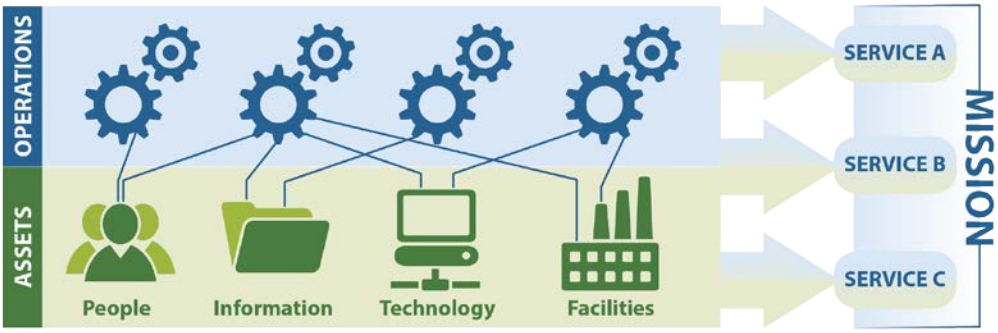
Critical Services

Critical Services	Examples of Supporting Assets
Water purification	Industrial control systems
Traffic control operations	Systems that manage traffic lights and cameras
Management of medical records for a health information exchange	Management systems and underlying architecture
State emergency management and coordination	Operations center and associated management systems

Homeland Security

**016 So just a slide that shows some example services. You know, water purification. Example assets on the right. That's a very basic slide just to kind of reinforce the point, right. State emergency management. Might have an operations center, and the management systems within the center and, you know, what else is needed to deliver information to who's important to receive it.

Identifying Critical Services: Summary



People – Are there leaders with cybersecurity responsibilities? (Cybersecurity Leadership)

Information – Is operationally sensitive information identified? (Information Protection)

Technology – Does the organization allow remote access assets? (Cybersecurity Controls)

Facilities – Does the organization have access to an alternative location? (Incident Response)

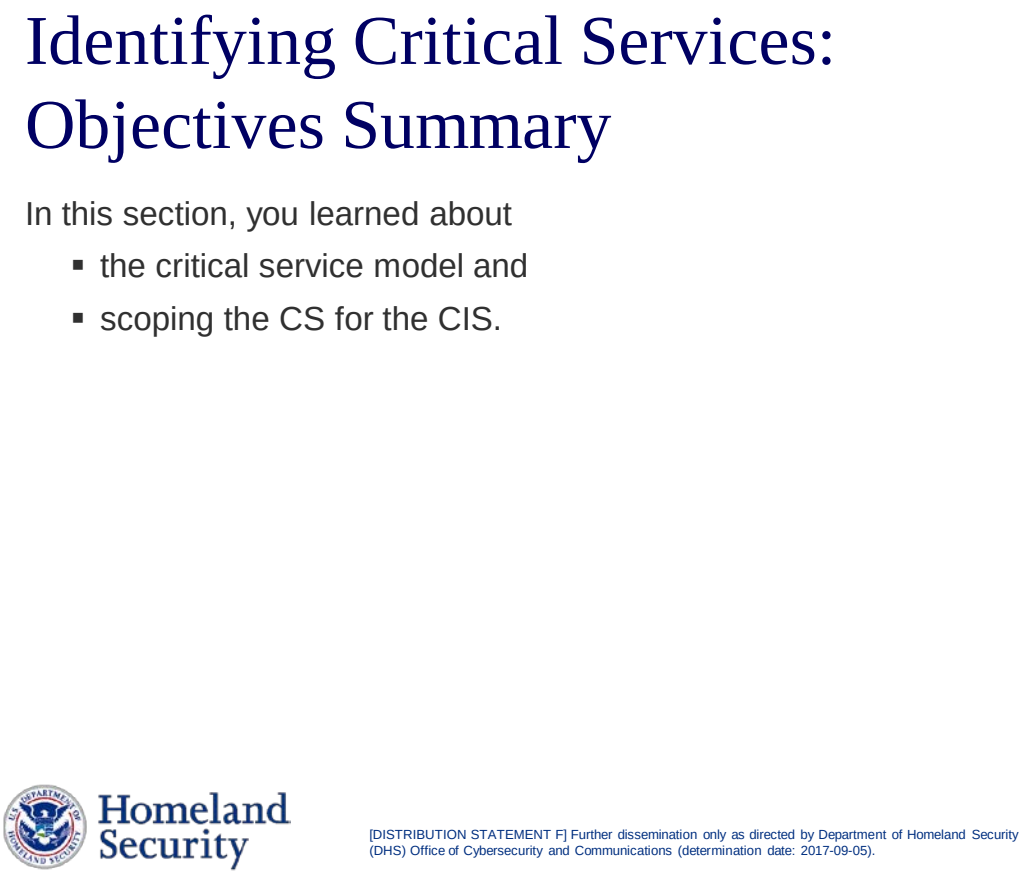
Homeland Security

**017 So in summary, you know, you want to scope the service. You want the service to be tied to the mission. It should be a high-value service. That's not to say that a printer may not ever be part of that, right. I mean, there's--you might run across a situation where there's a very high technology-based printer that's core to the service. Then it would be part of it.

General printing is not something you would normally consider, right. So again, the asset types that we focus on, people, information, technology and facilities. You want to define those as what's important to the service

and note that the CIS does have some aspects about facilities but it's not as prominent as some of the other assessments that you'll be doing.

Identifying Critical Services: Objectives Summary



**018 So in summary, you know, we review, you know, the critical service model and some of the aspects to consider while scoping the critical service for an organization. Any other questions before we conclude this?

If you have questions later, we can come back up and we'll take them then.

Introduction

Table of Contents

Administering the CIS

September 2017

Homeland Security

**001 Instructor: All right, this section is called Administering the

**002 [Notice]

Administering the CIS: Objectives

After completing this section, you will understand

- the types of questions in the CIS,
- the concept of least common denominator, and
- the intent of each CIS domain.

**004 So, the objectives of this section are going to be to identify the types of questions that the CIS asks. We're going to get into the concept of least common denominator. And we are going to start to give a high level overview of the intent and the types of concepts in each CIS domain.

Administering the CIS: Topics

Types of Questions

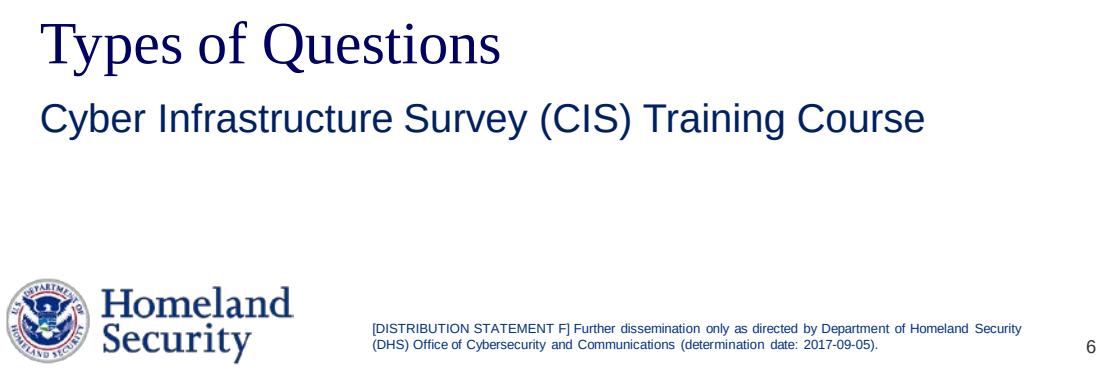
Least Common Denominator

CIS Domains

**005 So, again, this is broken up into three separate areas. We have the types of questions. We have a section on least common denominator and then CIS domains.

Type of Questions

Table of Contents



**006 So, types of questions.

Types and Numbers of Questions

Four Question Types

CIS Domain	Checkbox	If Yes	Text Input	Notes	Total
Background Information	27		35		**62**
Cybersecurity Management	28	47		22	**97**
Cybersecurity Forces	8	11		4	**23**
Cybersecurity Controls	24	55		16	**95**
Incident Response	9	7	1	4	**21**
Dependencies	5	36		8	**49**
Total	**101**	**156**	**36**	**54**	**347**

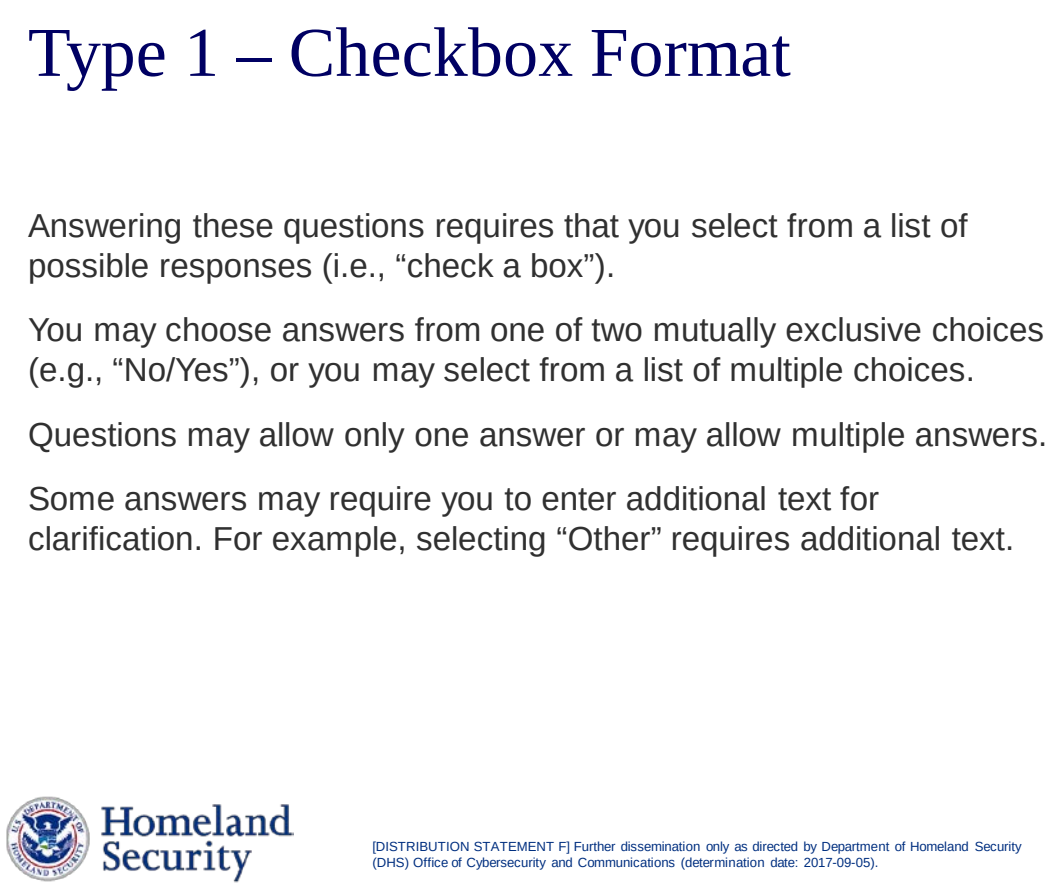
Homeland Security

**007 What you see here is a kind of overall summary of what the CIS and the question structure looks like. So, we show all of the domains and the totals. You can kind of get a sense for the larger domains. We have checkbox style questions.

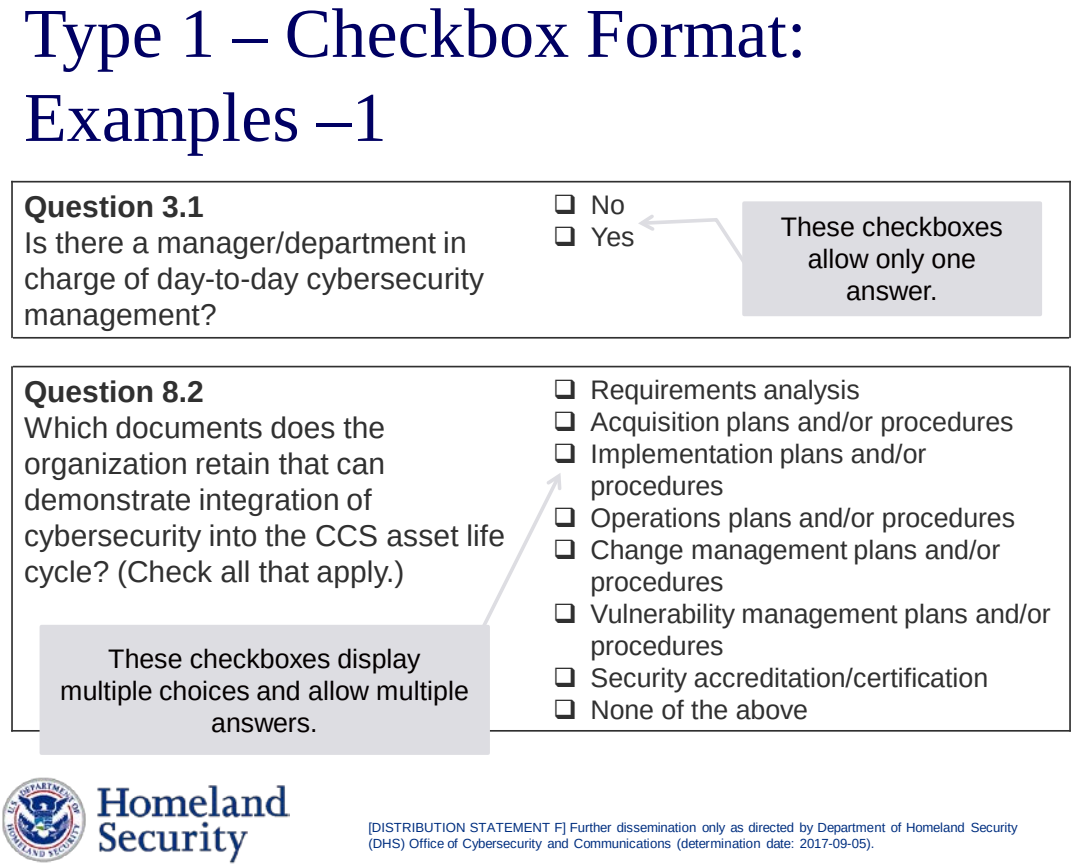
We have if/yes style questions. There's questions that offer text input. And then there's also notes. You can see that a vast majority of the domains focus on the checkbox and if/yes. So, while the text input is at the background information where you're gathering a lot of the information from the organization. But overall, you're going to be asking around

three hundred and forty-seven questions during the day.

Type 1 – Checkbox Format

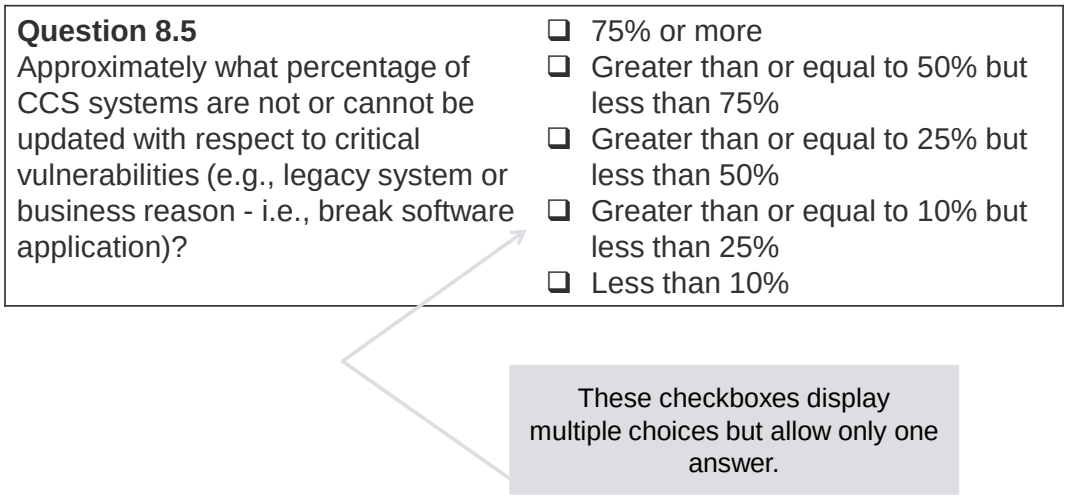


**008 So, the first type of question is checkbox format. These are you check a box type questions. Normally, you can choose between yes and no. These questions normally only allow one answer. But there are areas in the CIS where there's multiple checkboxes that can be selected. And then some questions, after you check the box, require you to do a text input as well. So, if you check other, you should clarify what that other is.



**009 So, here's some examples of just checkbox only. The top question is your standard yes/no question. The bottom question is checkboxes that allow multiple inputs. So, it's important in the CIS, where you can input many inputs to answer, everything that's applicable to the organization because each check is a weighted practice that can add or subtract from the CPRI score.

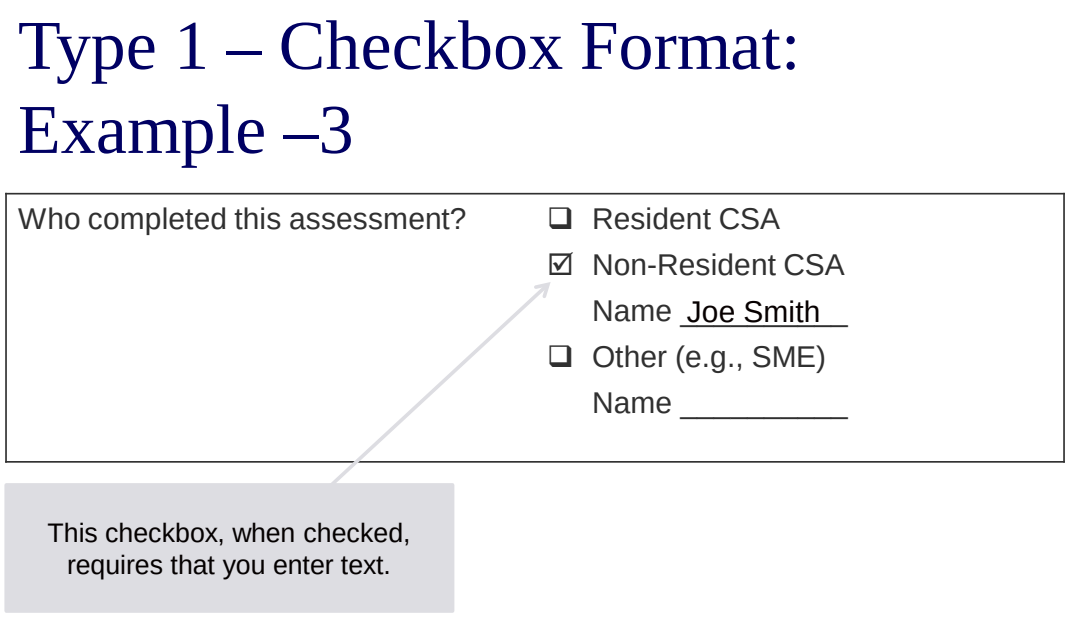
Type 1 – Checkbox Format: Examples –2



Homeland Security

**010 Example two would be a checkbox where there's more than just yes or no. But there's many options. But in this case, you're only selecting one checkbox. The CIS is pretty good about saying select all that apply as you're going through the question set but that's not always the case.

Type 1 – Checkbox Format: Example –3



**011 Example three, as I stated before, this would be a checkbox question. Any time there's further information required, best practice is to input that further information via text. So, non-resident CSA put the text of the name of the person.

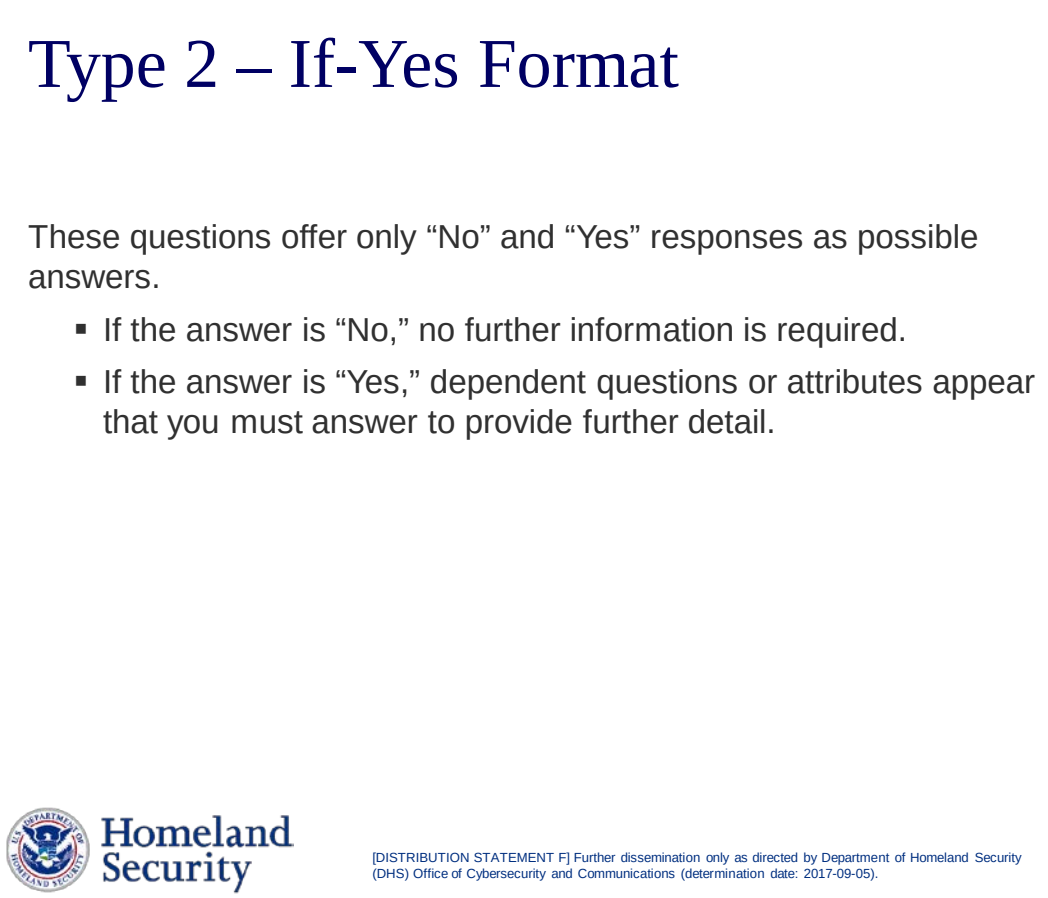
Instructor: Hey Gavin, if I could?

Instructor: Yep.

Instructor: One thing to note here is-- and the reason we're stating this-- it seems obvious. But this is one of the things that is kind of caught in QA, where many times there is something like this that should have

additional text, and it's really not specified. So, this is something to look for so that you don't miss that fact and add the additional information.

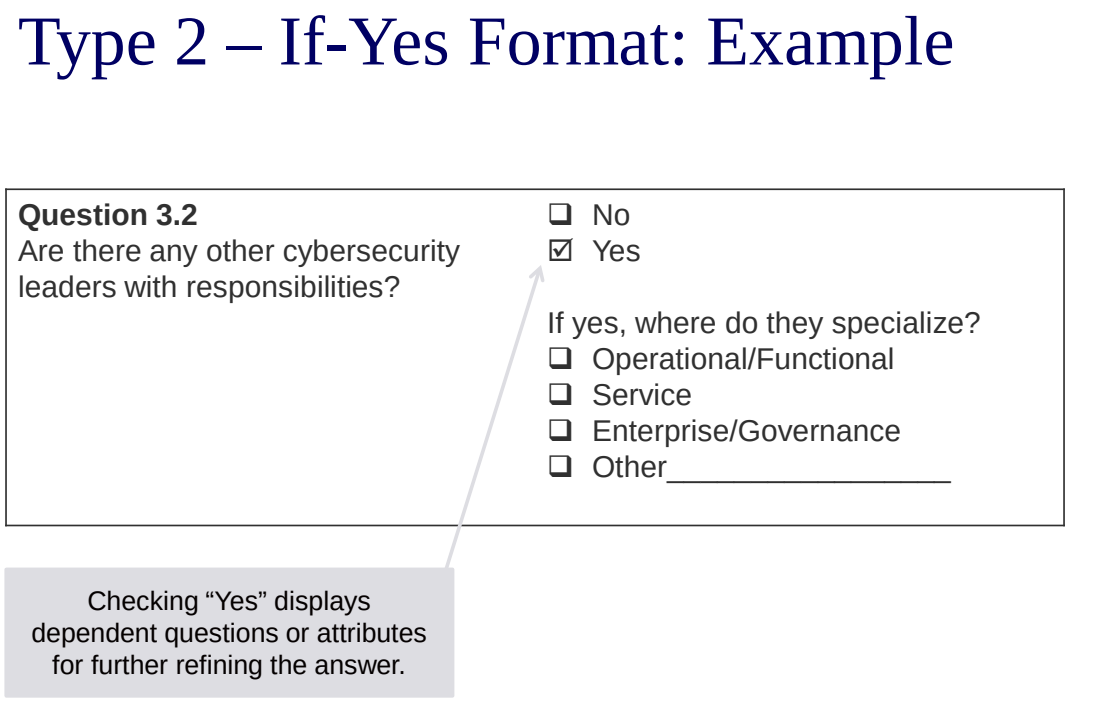
Type 2 – If-Yes Format



**012 Instructor: Okay the second type of question is if/yes format. Typically, these are checkbox type questions where you're asking about a practice. And if you select no, then no further information is required. But if you select yes, the survey will pop up with a lot more options that then you have to go down through the checkboxes and answer. So, pretty much if there's a yes, there's a

bunch of dependent questions that show up under that that you can drill down into more information.

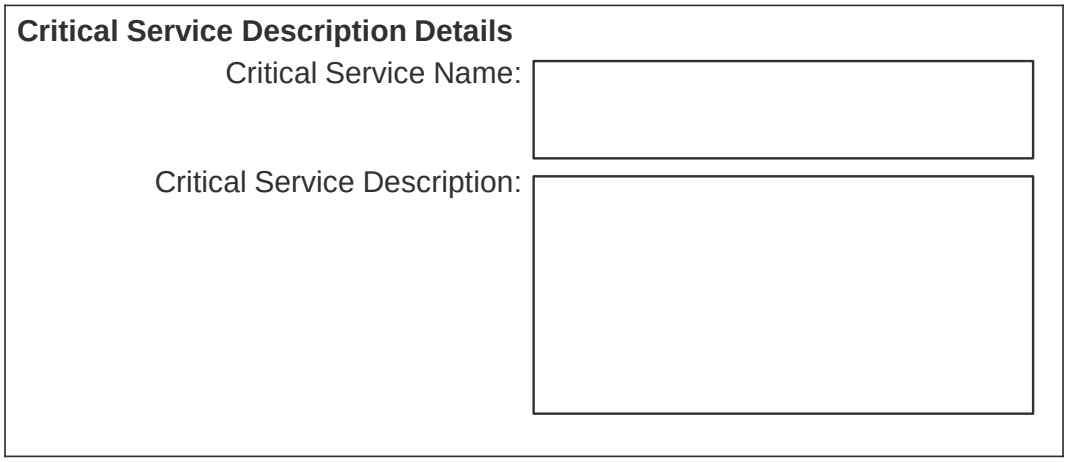
Type 2 – If-Yes Format: Example



**013 So, here's an example. In the CIS, you won't see the dependent question all the time right away. So, if you hit no, you may not necessarily see the if yes, what do they specialize in. If you hit yes, then that if yes, where do they specialize, you can select the appropriate answer then.

Type 3 – Text Input Format

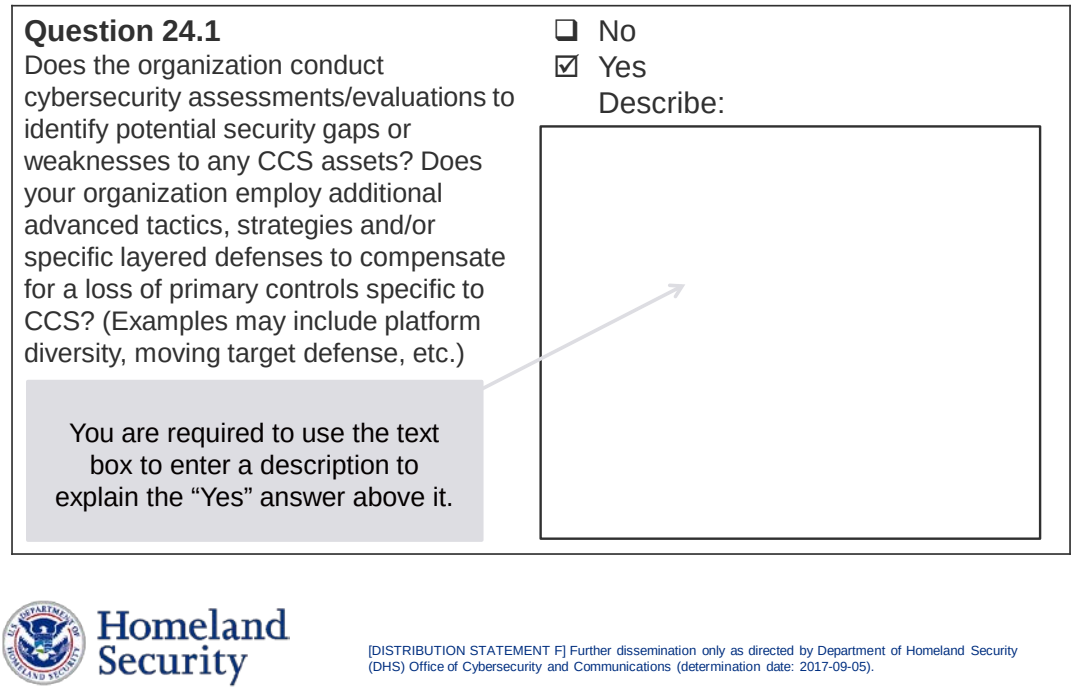
Text input questions require you to enter text and are used when qualitative data is needed or to allow you to respond in detail.



Homeland Security

14

**014 The third type of question format is text input. You'll find a lot of this in the background information section. So, for instance, this is where you just describe the critical service, the critical service description. As much text as you can put in is helpful because if you have to revisit the CIS a year later, obviously, the more information you have, the easier it is to recall the details of that engagement.



**015 Here's an example of the text format that's actually within the body of the survey. You're asking to do a checkbox type question and describing it. It's giving you a big text box to describe the information that's asked about in that question. The last--

Instructor: Hey, Gavin, could you go back? So, notice the call out box. Again, we've called this out multiple times because you're required to use the text box to enter a description. They're expecting that. It should never be blank in this case.

Type 4 – Notes Format

Notes are optional, free-form text fields you can use to record additional information.

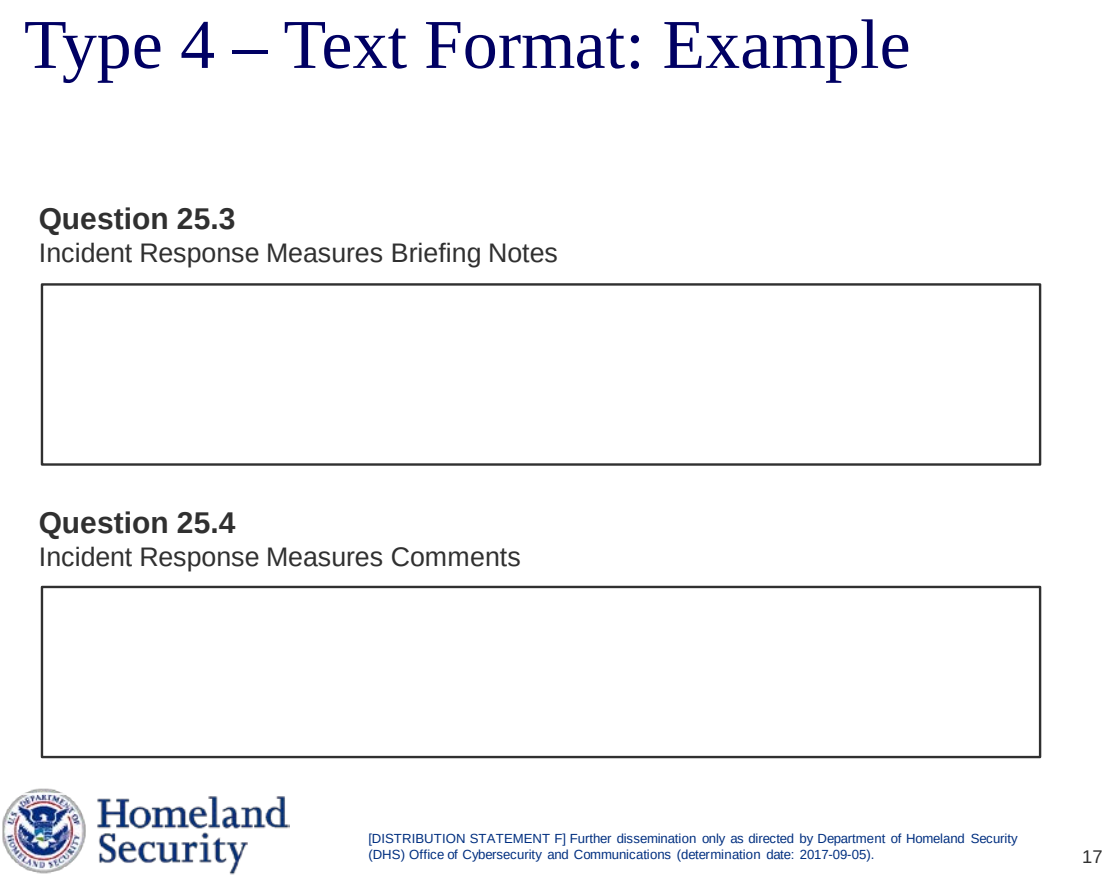
There are two types of notes:

- **Briefing Notes** are intended for the team and are not visible on the dashboard.
- **Comments** are intended for the CIS customer and are visible on the dashboard.

**016 So, the last type of question we talk about is the notes format. So, at the end of every domain, or actually every section of the CIS, you have an area for briefing notes as well as comments. The briefing notes, you want to know that they're intended for the team and not visible to the customer at the end of the engagement. So, because you normally are projecting the CIS on a screen while you're typing information in, they may or may not be able to see what you're putting in. But when you deliver the dashboard, they're not going to see the briefing notes. If you want the organization to see some comments that you've

captured from the point of contact or whoever was in the engagement, you want to use the comment field. That will show up in the dashboard after delivery.

Type 4 – Text Format: Example



**017 This is typically how you'll see them. They're at the end of every section. A little later on in the training, whenever we're doing the facilitation, we give tips on exactly the type of comments you would want to capture, some tips for the briefing notes as well.

Least Common Denominator

Table of Contents

**018 Okay, that ended the types of questions. We're going to talk about least common denominator now.

The Weakest Link

A cybersecurity program is only as strong as its weakest practice.

Always select the response that represents the lowest level of execution or implementation for the organization.

Be aware of and only answer the question as it relates to the part of the service that represents the least effective implementation of the practice.

To ensure the most accurate response, consider different parts of the CS.

If an organization is not doing the practice anywhere, the answer should be “No.”

**019 So, as we discussed during critical service, there's many, many different aspects to a critical service, many different assets that you're going to be talking about. You really want to keep in mind the weakest link whenever you're doing this. So, typically when you ask about a practice, what I've always found is somebody always has their gold standard in mind. Oh yes, we do this for this particular asset type or these documents. But if you kind of tease more information out-- okay, well you're doing this really well. What about this other aspect of the critical service? Are you doing this here? You want to make sure that you're really

only answering some of these questions for the weakest link and not giving them more credit than credit is due.

So, a cybersecurity program is only as strong as the weakest practice. You're going to want to select the responses that represent the lowest level of execution or implementation. And we are going to go through a couple examples and see how we would answer those. So, be aware of and only answer the question as it relates to the part of the service that represents the least effective implementation. And again, a good tip is don't accept just the first answer they give you. Kind of tease the different aspects. As you're going through the assessment, you're going to become more familiar with their systems and stuff, too. So, you can start to ask more questions and challenge them a little bit on-- and try and get the most accurate responses. If an organization is not doing the practice anywhere, then the answer should be no.

Least Effective Implementation: Three Examples

We present examples of least effective implementation from

- Change Management
- Cybersecurity Exercises
- External Information Sharing

Homeland Security

**020 So, least effective implementation, we're going to go through three different examples. The examples are going to come from change management, cybersecurity exercises, and the external information sharing.

Change Management

7.1 Which option best describes the organization's approach to cyber change management (e.g., new hardware/software, employee access)? *(Check one)*	☐ Has revision logs documenting who made the changes to a policy, procedure, plan, inventory or architecture documentation and incorporating a brief synopsis of the change and the corresponding date of those changes; this would include a backout plan. ☐ Has a documented and distributed cyber change management policy and supporting procedures. ☐ Has documented and distributed change management procedures. ☑ Has an ad hoc process for regulating and approving changes. ☐ Does not do change management.

The organization provides the following responses:

- To change an employees access levels, everyone knows that the manager of the system needs to be emailed.
- Any changes to hardware are submitted via the change management process and reviewed by the change control board.
- Software is strictly version controlled with detailed revision logs.

How would you record the organization's response?

**021 So, throughout the course of an assessment, you're going to get the change management in question 7.1, which asks, "Which option best describes the organization's approach to cyber change management? For example, their new hardware/software, employee access." You have a bunch of options you can select to the right that they may or may not be doing for each asset type or different assets within the organization.

So, during the survey, we get the following responses from the organization. So, they say to change an employee's access level, everyone knows that the manager of the

system needs to be emailed. When you start to ask about hardware, they say any changes to hardware are submitted via the change management process and reviewed by the change control board. And with software, it's strictly version controlled with detailed revision logs.

So, that being said, you've asked about employee screening. You've asked about hardware. And you've asked about software. How would you record the organization's response to this question? Any takers?

Student: I'd go with the first bullet, seeing how that's the least of the three.

Instructor: So, the revision logs would be the most. So, for hardware, they're doing the most actually for hardware and software. So, I would argue that you would have an ad hoc process because when you're accessing about employee access and how they're requesting, if an employee needs access to different levels or different systems, they're telling you we don't really have a process for that. He's just saying, "You know, everyone should know that they need to ask the manager." And these are kind of the little idiosyncrasies that happen whenever you're doing an assessment. You really want to-- if they said they have a procedure, we could probably go up a step. But it's really ad hoc. From our information, we don't know if every employee knows that. We're just taking someone's word. So, for

this, the least effective implementation would be for the employee access levels, where they are-- it's an ad hoc process. They're doing pretty good for hardware and software. That seems to be strictly version controlled, change management, and whatnot.

Instructor: So, the point is the reason we're emphasizing this is that the way the CIS is structured, it's expecting the lowest or the least effective implementation to be put in as the answer. It's looking at it as I'm not going to give credit for what you might be doing over here in a great way. I'm going to be saying what's happening across your entire service. And I'm going to be picking the least effective implementation of that as it applies to the service because it's really trying to account for that weakest link and not give anybody a false sense of security that everything is way up here. When in reality, you have to consider that whole service. And that weakest link is way down here.

Instructor: And conversely, if we think about the CRR then, we ask about specific asset types. So, for people, this may be answered incomplete. But the would get a yes, they're doing this practice for--

Student: This is where I-- because when I do a CIS, I'm looking for not just am I doing it for them today, but if I'm going to come back and do one for them next year, using the comment section very heavily saying

they did really well here and here. This is the reason I'm scoring them lower than they should. And this is the area that they-- if they need to improve upon, or can show me next time I come out, that will get them a higher score.

Instructor: Right.

Student: That's what I'm using the comment section really for because there is no way, like you said earlier, there's not a report that's generated out of this or to show you why something was scored low. So, if I want to track based on future engagements with them, you've got to use the comment section for that.

Student: Yeah, I always try to give them as much credit as they can while being true to the intent of the question. I do the same thing, use the--

Instructor: And even comments like this, maybe not worded this way, but something like that to go back to and refer to why you answered at a lower level than that. That's good to have.

Student: Does it go in your comments or the briefing notes?

Student: If you want the customer to see it, put it in the comments. And usually the customer is asking saying, "Can you make a comment on that for me so I know what to go back in and fix, or why I'm scoring a little lower here." So, I don't use the briefing notes a whole lot. I use the comments section a lot though.

Student: I would agree with that.

Instructor: The briefing notes are really for you internally. You might put additional information there to substantiate what you've done so that you have it during a debrief.

Instructor: Right.

Instructor: You may take some of their comments based on maybe how some of the questions are architected or something like that. And we'll be going over more of that in a later section.

Instructor: Yeah.

Student: I use the briefing notes if I'm answering a reason for quality assurance when they're double-checking why I answered a question this way if I answered another question differently early on. I'll put that note in there saying, "I answered it this way. I'm allowing this answer here even though questions number one back there said this. This is why I'm qualifying this one here." So, to get through Q and A.

Student: Especially if they're in progress with something, they know that they're working on something. And they're six months out or something like that. That's a good place. You can put in the comments that-- ultimately, the way I look at it, it's for their benefit. And if they have a comment in there that they feel helps them maybe up with

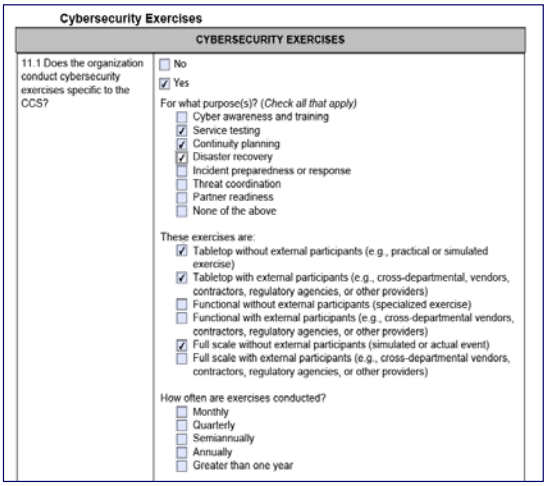
management, or within their own organization, I really try to capture that.

Instructor: Okay. Great.

Cybersecurity Exercises –1

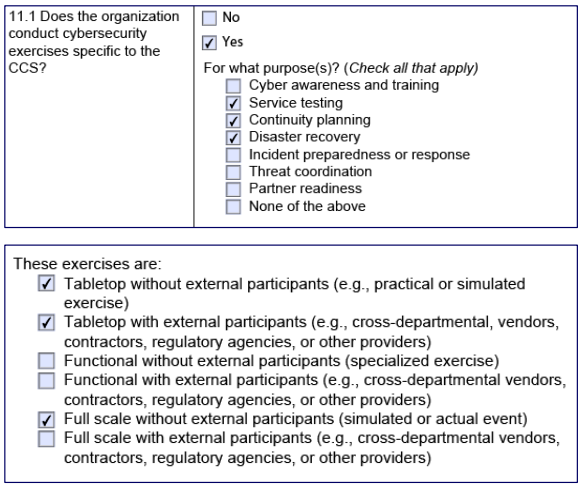
Cybersecurity Exercises –1

The organization provides the following responses to Question 11.1:



Cybersecurity Exercises

CYBERSECURITY EXERCISES	
11.1 Does the organization conduct cybersecurity exercises specific to the CCS?	☐ No ☑ Yes
For what purpose(s)? (*Check all that apply*)	☐ Cyber awareness and training ☑ Service testing ☑ Continuity planning ☑ Disaster recovery ☐ Incident preparedness or response ☐ Threat coordination ☐ Partner readiness ☐ None of the above
These exercises are:	☑ Tabletop without external participants (e.g., practical or simulated exercise) ☑ Tabletop with external participants (e.g., cross-departmental, vendors, contractors, regulatory agencies, or other providers) ☐ Functional without external participants (specialized exercise) ☐ Functional with external participants (e.g., cross-departmental vendors, contractors, regulatory agencies, or other providers) ☑ Full scale without external participants (simulated or actual event) ☐ Full scale with external participants (e.g., cross-departmental vendors, contractors, regulatory agencies, or other providers)
How often are exercises conducted?	☐ Monthly ☐ Quarterly ☐ Semiannually ☐ Annually ☐ Greater than one year



11.1 Does the organization conduct cybersecurity exercises specific to the CCS?	☐ No ☑ Yes
For what purpose(s)? (*Check all that apply*)	☐ Cyber awareness and training ☑ Service testing ☑ Continuity planning ☑ Disaster recovery ☐ Incident preparedness or response ☐ Threat coordination ☐ Partner readiness ☐ None of the above

These exercises are:
- ☑ Tabletop without external participants (e.g., practical or simulated exercise)
- ☑ Tabletop with external participants (e.g., cross-departmental, vendors, contractors, regulatory agencies, or other providers)
- ☐ Functional without external participants (specialized exercise)
- ☐ Functional with external participants (e.g., cross-departmental vendors, contractors, regulatory agencies, or other providers)
- ☑ Full scale without external participants (simulated or actual event)
- ☐ Full scale with external participants (e.g., cross-departmental vendors, contractors, regulatory agencies, or other providers)

Homeland Security

22

**022 Okay. So, the next example has to deal with cybersecurity exercises. So, you get to question 111.1. You ask, "Does the organization conduct cybersecurity exercises specific to the critical service?" They say, "Yes we do. We do service testing. We do continuity planning. And we do disaster recovery." Furthermore, they're saying, "These exercises, we're doing tabletop with

external participants. We're doing tabletops with internal participants. We're doing full-scale without external participants, as well.

The follow on question to this is, "How often are exercises conducted?"

Cybersecurity Exercises –2

Cybersecurity Exercises –2

The organization provides the following responses:

- Tabletop cybersecurity exercises without external participants occur quarterly.
- Tabletop cybersecurity exercises with external participants are supposed to happen annually, but don't always occur.
- Full-scale cybersecurity exercises occur annually.

How would you record the organization's response?

How often are exercises conducted?
- ☐ Monthly
- ☐ Quarterly
- ☐ Semiannually
- ☐ Annually
- ☑ Greater than one year

Homeland Security

23

**023 So, they respond, "Well, we do tabletop cybersecurity exercises with external participants quarterly. Tabletop cybersecurity exercises with external participants are supposed to happen annually but don't always occur. And full-scale cybersecurity exercises occur annually." How would you answer

this question? What's the weakest link?

Instructor: Yeah. So, even though some of them, they're doing good, you have to take into account the least effective implementation.

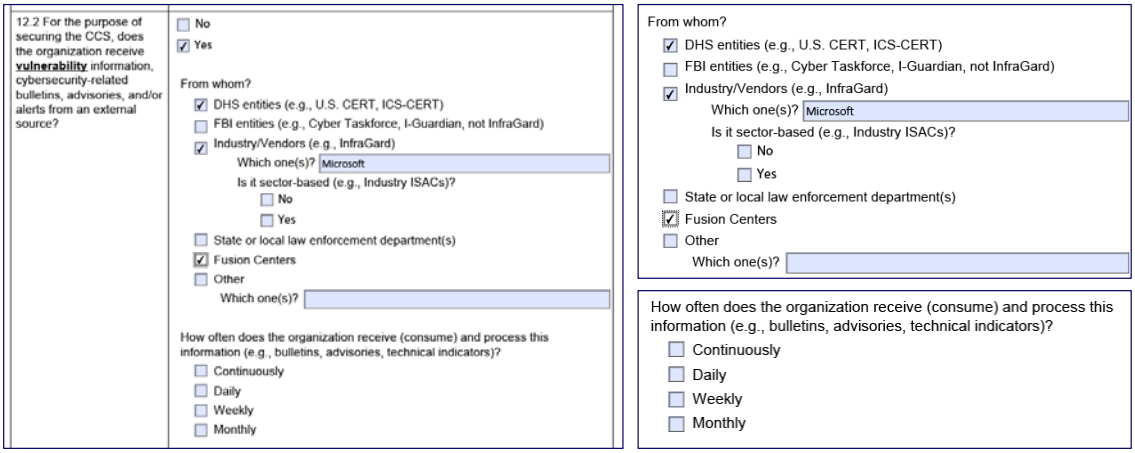
Student: And that's where you could use the comments to spell that out, what they do.

Instructor: Correct.

External Information Sharing –1

External Information Sharing –1

The organization provides the following responses to Question 12.2:



Homeland Security

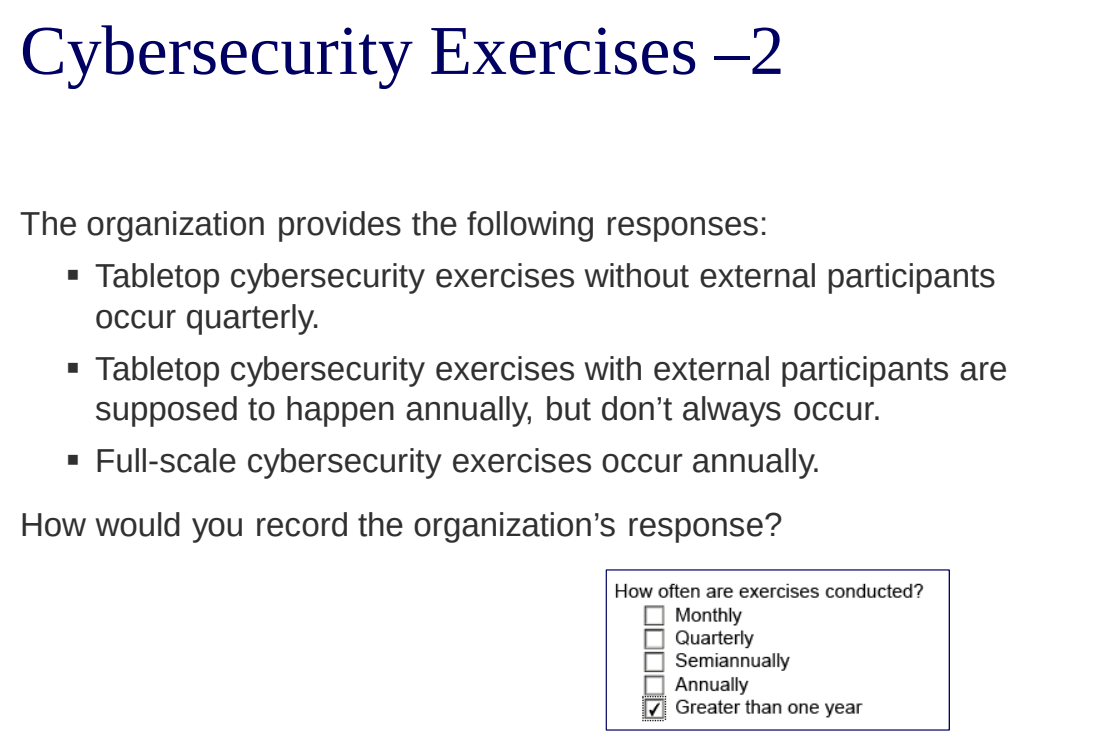
**024 Instructor: So, you need to keep in mind that the CIS is architected this way. So, you need to

take that approach throughout the assessment.

Instructor: Okay.

Student: Can we go back one real quick?

Cybersecurity Exercises –2



**023 Instructor: Sure.

Student: Okay. I think I've been doing that wrong. So, that's a good-- so, anything that they checked in the box before, you need to kind of ask the question again. So, how often are you doing this one? How often are you doing this one? How often are you doing this one?

Instructor: Right because this one is kind of a roll up of all of them.

Student: Okay.

Instructor: So, they're saying they're doing three different-- if they're only doing one, then obviously this is a one-to-one mapping. But because they're doing three different types, and they're doing all those different exercises, you have to take into account the least effective one that they're doing.

Student: Okay.

Student: You're not the only one, Klint.

Student: Well, and I'm just thinking though. So, if a customer then looked at you and said, "Okay, sometimes I do tabletops. But I do an annual exercise every year." So, if they told you those things, and you mark the two boxes, they do tabletops and annual exercises. Now, you have to score them on this box here that it's greater than one year because sometimes they do it. Or but if you just said okay, they don't do-- we'll just exclude tabletop exercises. Then you're doing a one-for-one. You could say annually. So, how does that change the scoring depending on whether they were up front with you, or if you decide to-- since it's an ad hoc exercise or tabletop thing, if you just didn't score them on that at all, is that really skewing the scores overall? Would we be better off not answering it that way, or--?

Instructor: I think it's best to just be an honest approach because you don't know if, within your organization, that they believe they are doing tabletops in addition to this annual test because the tabletops may be focused on different aspects. But the organization may not know that it's really not happening the way they expect it is. Now, they would know that. And you can put in your comments that this portion is being done annually. But however, the tabletops are being done at this frequency. And if it's expected that they should be done more, that's not happening.

Student: I would just drill down and ask them, "All right, you do tabletops ad hoc. Is it in excess of a year in between tabletops or not?"

Instructor: Yeah.

Student: If it's not-- they might do them ad hoc, but if they do three or four a year, then they're greater than annually.

Instructor: Yes.

Student: I've definitely been scoring that one wrong.

Instructor: This is a-- just like the other assessments, it's a point in time assessment like what are they doing today I've seen where management has one set of expectations of what they believe is happening. And what's really happening, for whatever

reason, isn't that. This would allow that to come out.

Student: So, just to pile on that, I also do it the other way around because I'm projecting that up there. And then as soon as I say greater than one year, they'll say no, I'm providing that on a quarterly basis. It just says how often are exercises conducted. And the partner will then say, "Well, it's quarterly." So, it will take--

Instructor: If it was one type, yes.

Student: Well, but that's-- it's like I'll have to go back to question design.

Student: Yeah, it's going to take some explaining on our part.

Instructor: Yeah, exactly.

Student: Now that we understand it, I think it will be easier for us to do it.

Student: Well, I wasn't doing it that way. I was asked how often do you conduct it. I would have said quarterly.

Instructor: Yeah. So, the way it's constructed today is you have to be cognizant of this.

Instructor: Because again, they're going to go to their best implementation right away.

Student: Well, of course they are.

Instructor: Yeah, so--

Student: It might be worthwhile to put that--

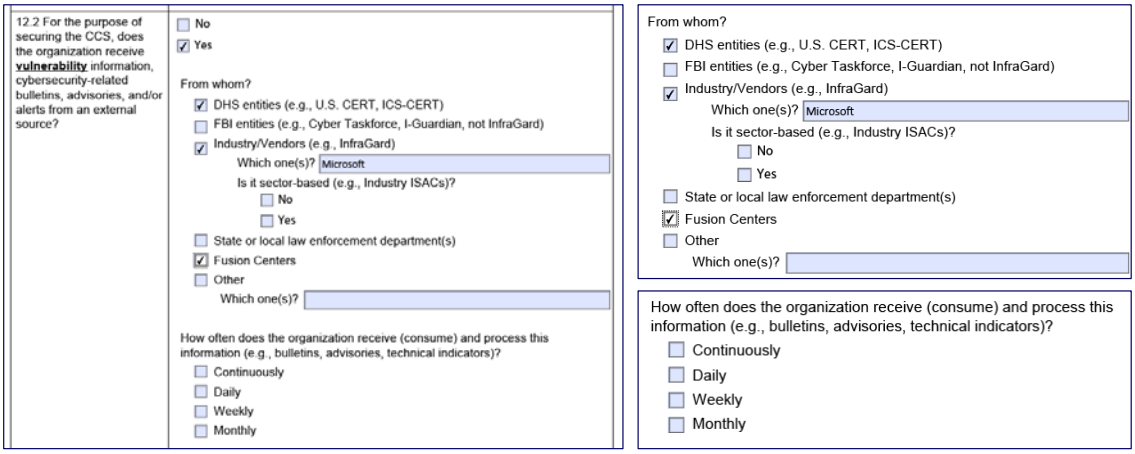
Student: They want a green.

Student: Under the checkbox that you say yes to.

Instructor: And that-- yeah, that's the way this is-- the questions are architected. In the other assessments, we have a little more leeway because we asked the same question four different ways where you can kind of capture some different aspects of that. But this, they could have been doing all seven different exercises. That might be too much to do effectively every year, too. But all right, the last example for this is in external information sharing.

External Information Sharing –1

The organization provides the following responses to Question 12.2:

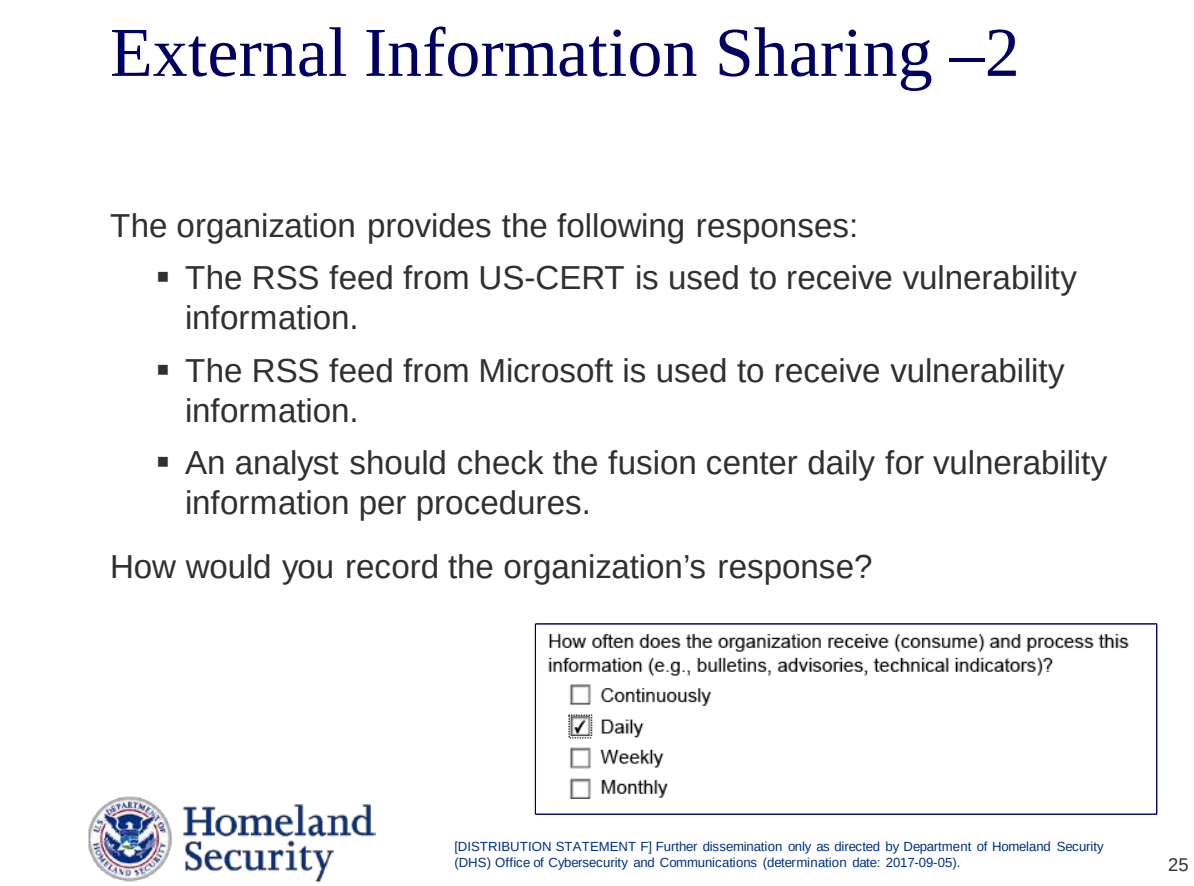


Homeland Security

[DISTRIBUTION STATEMENT F] Further dissemination only as directed by Department of Homeland Security (DHS) Office of Cybersecurity and Communications (determination date: 2017-09-05).

24

**024 So, if you get to 12.2, you ask, "For the purpose of servicing the critical service, does the organization receive vulnerability information, cybersecurity related bulletins, advisories, and/or alerts from external sources?" So, they say, "Yes we do. We receive it from DHS. We do industry vendors such as Microsoft. We also get alerts form the fusion center." So, then the follow on question to that is, "How often does the organization receive or consume and process the information from these bulletins, advisories, and technical indicators?"



**025 They say, "Well, we have an RSS feed from U.S. Cert. So, we receive that vulnerability information automatically, same with Microsoft. We also have an analyst that should check the fusion center daily for vulnerability information per procedures." So, how would you record the response for this?

Student: Weekly.

Student: Yeah.

Student: Define should.

Student: Yeah.

Student: Are you saying that he's not? He's not. Okay, so then--

Instructor: No, no, no, I'm-- don't-- I didn't say anything.

Student: I mean that's tough because you have the RSS feeds. How often-- is that a continuous thing because you signed up? So, I have a subscription. So, that's continuous in my view. I mean--

Student: But you're looking for the least.

Student: But that's my point. So, is that how we should be interpreting an RSS feed, as continuous? Or is it--

Student: Yes.

Student: Yes.

Student: That's continuous. The question is the analyst doing what he's supposed to do on a daily basis?

Student: That's-- right.

Student: That's-- you'd have to clarify that. He should be. What is he doing?

Student: Yeah, I put down daily.

Instructor: So, I would say daily here--

Student: The third bullet on that one, yeah.

Instructor: Because they said they have procedures. So, if the manager just said he should be doing this daily, and it's just part of his job description, I'd probably go weekly or longer. We have no way. But because he's saying that we have a procedure that says this person should be doing this daily, I would tend to record the answer based on per procedure. There's no way we can go in and tease whether everyone's following every procedure. But they have a written document that says this is your job description to do this daily. And that would be the least common implementation of that.

Student: See, I would have said weekly and put in the comment that they have a procedure. And the analyst should be doing it. But there's no confirmation that he is.

Instructor: So, Gavin did a good job with these examples because it's purposely not meant to be cut and dry. So, because there is a procedure involved, and that's what he should be doing-- because you may be in front of somebody that says, "I know there's a procedure. That's what he should be doing. So, it's happening on this frequency. But I'm not the person responsible for checking." He's giving you an honest answer of what should be happening. And he-- even if you dig rich, he may not be able to say. Just like I told you, I'm not the guy actually checking. But I know we have a procedure. And it should be done at this frequency. So, I--

Student: I'm not arguing. I'm not trying to-- I'm just saying if I was doing the assessment, prior to this, that's what I would have done. I would have checked weekly and made a comment.

Instructor: No, I think it's good. I think the comments are good because it's this discussion that's going to help everybody. I'm just pointing out the fact that in a lot of these answers there are going to be some gray areas you're going to have to get to the best understanding you can.

Instructor: Yeah, and in your specific scenario, so, if they had-- if you had the manager that says, "We have a procedure for this," but then they have the actual analyst in there saying, "Well, it says it in the procedure, but I'm not doing that," then you could put that in comments and check weekly.

Student: Or if you knew that there was only one analyst, and you have to realize that he has to take vacations and sick days and stuff like that--

Instructor: Yeah.

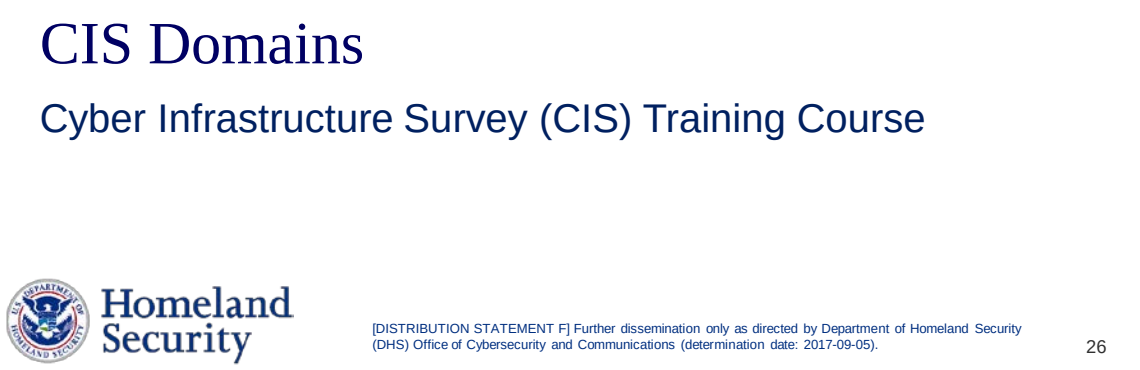
Student: They don't have a backup for that position.

Student: Yeah, I try not to read deeply into the-- you can drive yourself nuts going too deep into the question. But that's what I would have done prior to this shall we say.

Instructor: Okay.

CIS Domains

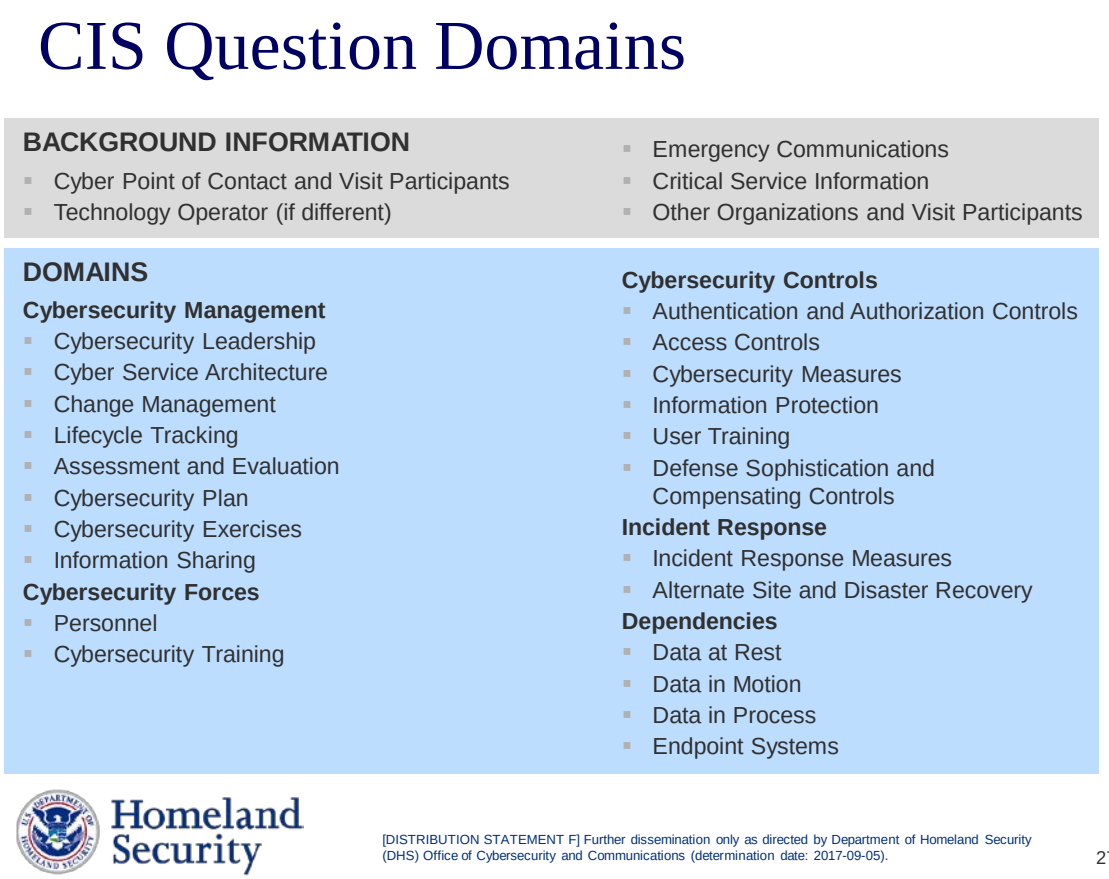
Table of Contents



**026 So, those were the examples for least common denominator. It's just something to keep in mind throughout the whole survey because you're asking a lot of-- you're asking for a lot of information. And, like we said, people tend to gravitate towards the best things that they're doing. So, you want to make sure to ask about the different aspects.

So, now we're going to kind of give a high level overview of the different CIS domains and the different topics that you can expect to find in those domains.

CIS Question Domains



**027 Again, here's how the CIS is structured. We're going to focus on the blue domains for the most part here.

Domains by the Numbers

Domain	Checkbox	If Yes	Text Input	Notes	Total
Background Information	27		35		**62**
Cybersecurity Management	28	47		22	**97**
Cybersecurity Forces	8	11		4	**23**
Cybersecurity Controls	24	55		16	**95**
Incident Response	9	7	1	4	**21**
Dependencies	5	36		8	**49**
Total	**101**	**156**	**36**	**54**	**347**

**028 Again, high level overview, you're going to be asking around three hundred and fifty questions throughout the day or half day.

Background Information Domain

Background Information Domain	Checkbox	If Yes	Text Input	Notes	Total
Cyber POC and Visit Participants	6		22		**28**
Critical Service Information	21		13		**34**
Total	**27**		**35**		**62**

This domain describes the organization. Specifically, it provides information about the

- primary cyber POC and other participants and
- critical service (CS), including site information, service demographics, and service composition.

**029 Background information is broken down as such. You're going to be capturing information about the primary point of contact. You're going to be capturing information about the critical service, site information, service demographics, service composition. So, there's areas to put here's the servers, here's the different networking components in there. The more information the better.

Cybersecurity Management Domain

This domain describes leadership roles and responsibilities (e.g., governance), documentation, lifecycle tracking, information sharing (e.g., threat information), accreditation, assessment, and audits.

Cybersecurity Management Domain	Checkbox	If Yes	Text Input	Notes	Total
Cybersecurity Leadership	4	2		2	**8**
Cyber Service Architecture	3	9		6	**18**
Change Management	4			2	**6**
Lifecycle Tracking	6	2		2	**10**
Assessment and Evaluation	2	9		2	**13**
Cybersecurity Plan	2	6		2	**10**
Cybersecurity Exercises	1	6		2	**9**
Information Sharing	6	13		4	**23**
Total	**28**	**47**		**22**	**97**

Homeland Security

**030 Cybersecurity management domain, so there's ninety-seven total questions here. I believe this is the biggest domain of the CIS.

Cybersecurity Leadership

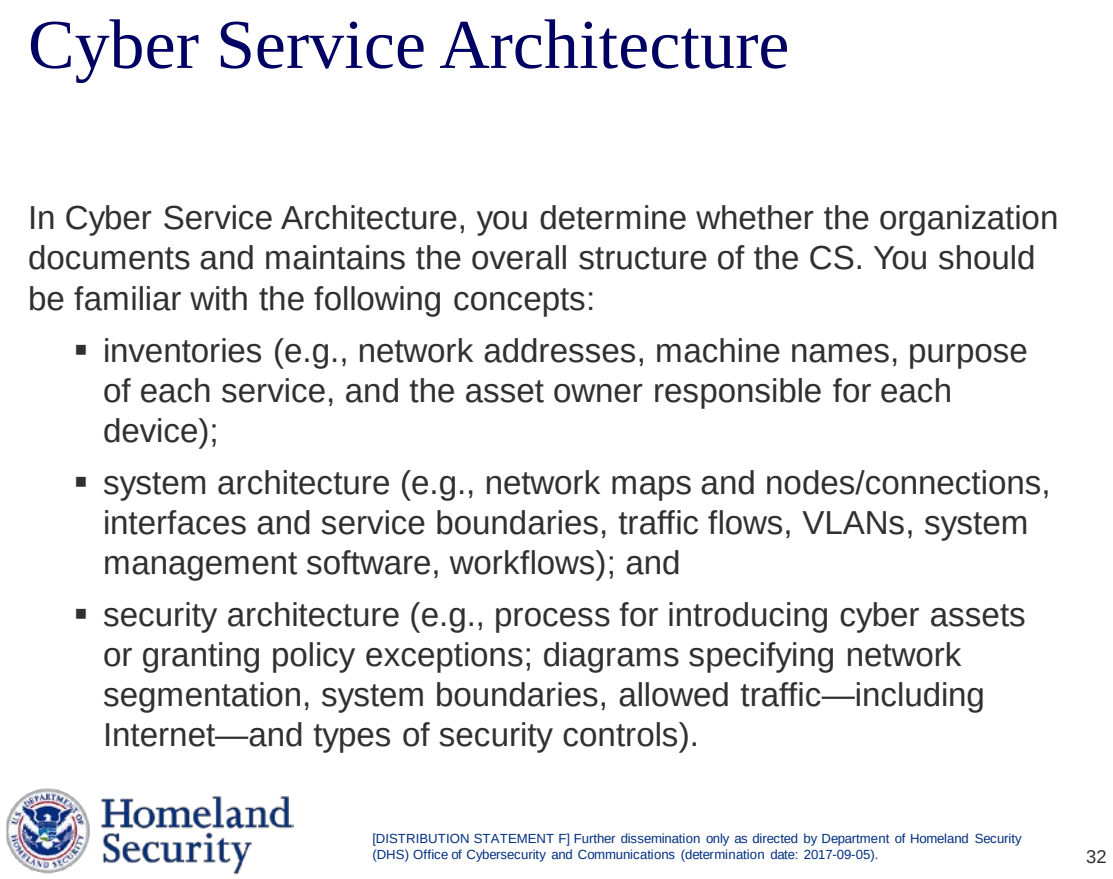
In Cybersecurity Leadership, you identify whether the organization assigns responsibilities for the overall cybersecurity of the CS. You should be familiar with the following concepts:

- managing day-to-day cybersecurity tasks;
- assigning responsibility at the operational, service, and enterprise levels; and
- managing vendors and third-party contractors the organization depends on for outsourced cybersecurity needs.

**031 And we're going to start with cybersecurity leadership. So, in this domain, you're going to identify whether the organization assigns responsibilities for the overall cybersecurity of the critical service. So, as a CSA, in doing this domain, you should be familiar with how to manage day-to-day cybersecurity tasks, how you would assign responsibility at operational, service, and enterprise levels, and then as well as managing vendors and third-party contractors. So, within this domain, you're going to be asking about this stuff. Once you ask the question-- for the newer CSAs, you ask the question, and then you're

kind of in the spotlight. And you have to provide examples to further explain what you mean. Here's the stuff that you should be familiar with for this domain.

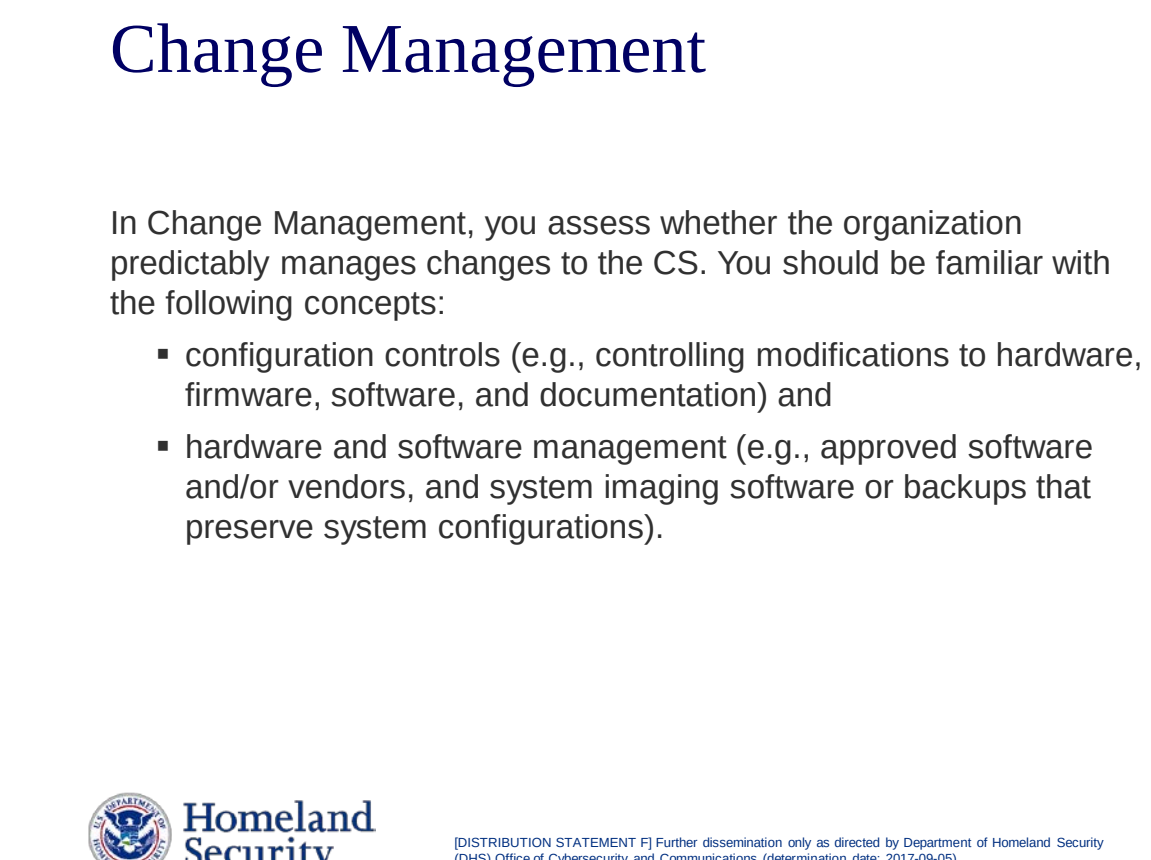
Cyber Service Architecture



**032 The next subdomain would be cyber service architecture. So, you're going to determine whether the organization documents and maintains an overall structure for the critical service. So, you want to be familiar with inventories. How do you inventory the different network addresses, the different technology? You want to be familiar with system architecture. What consists of a

system architecture? So, network maps, nodes, connections, traffic flows. And then to build on that system architecture, what is a security architecture? So, do you have defense in depth model? Do you have different segregated networks? You want to know about all these concepts so you can explain maybe even some best practices if they're not doing some of these. Any questions on this?

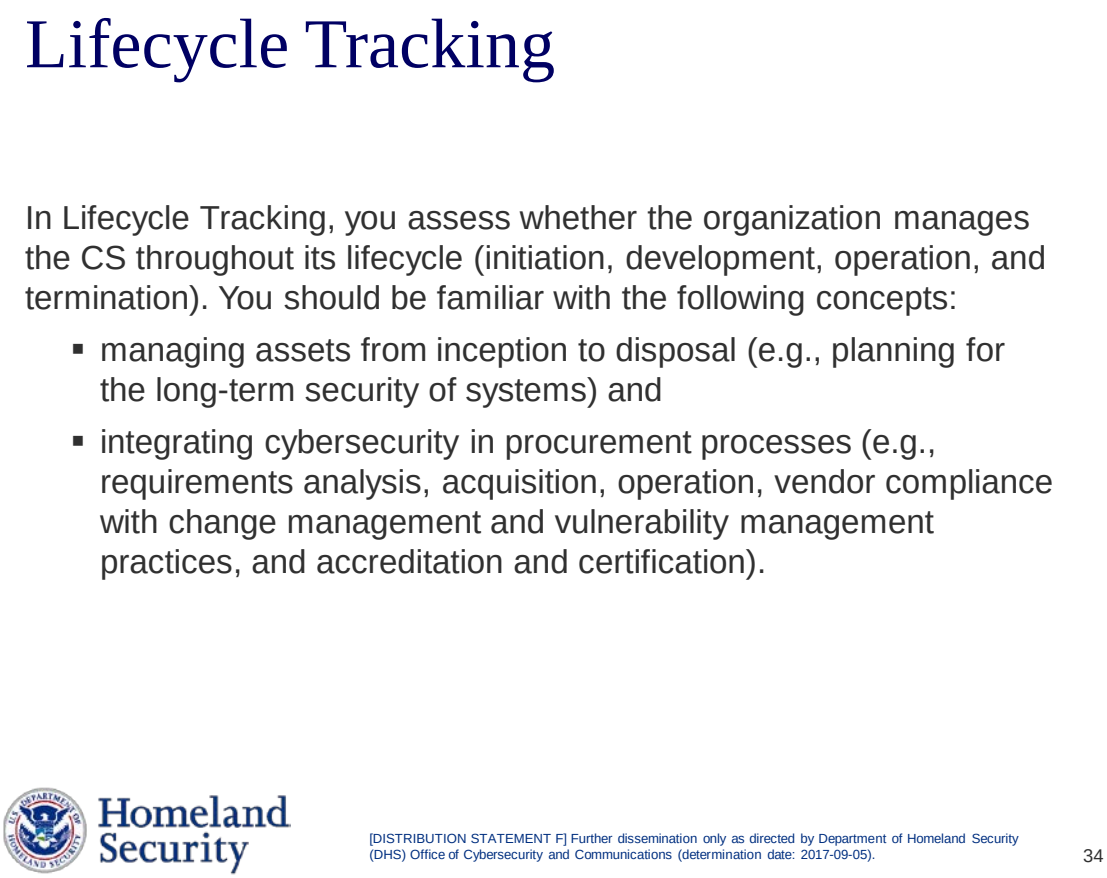
Change Management



**033 Then we get into change management. So, we're going to assess whether the organization predictably managed changes to

assets for the critical service. You should be familiar with configuration controls, hardware and software management, different things like that. So, change control boards, change control procedures, you're going to be asking about that in this section.

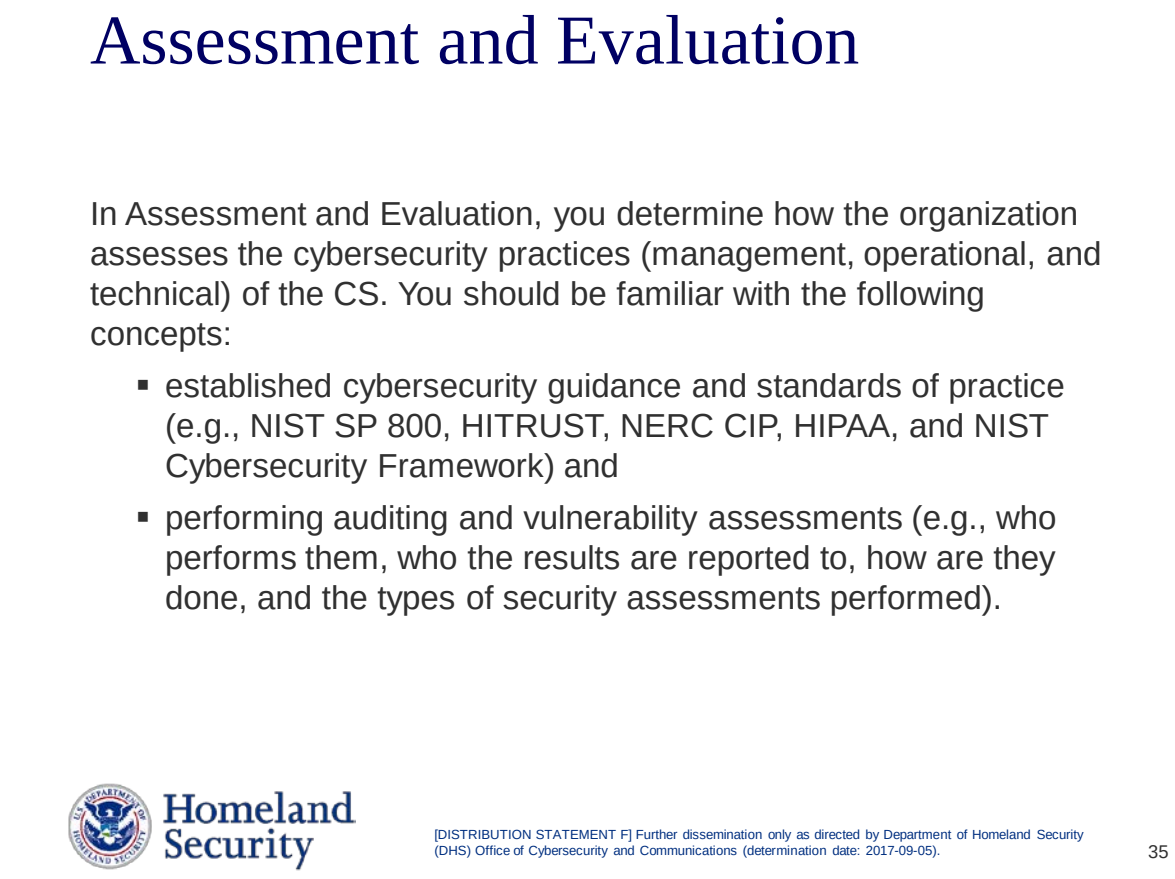
Lifecycle Tracking



**034 We then get into the lifecycle tracking. So, you assess whether the organization manages the critical service throughout its lifecycle, which would be initiation, development, operation, termination. There's a bunch of different lifecycles and different phases out there. But you're

really seeing if the organization uses the lifecycle approach. So, managing assets from inception to disposal and integrating cybersecurity into the procurement processes in the different design phases, implementation phases.

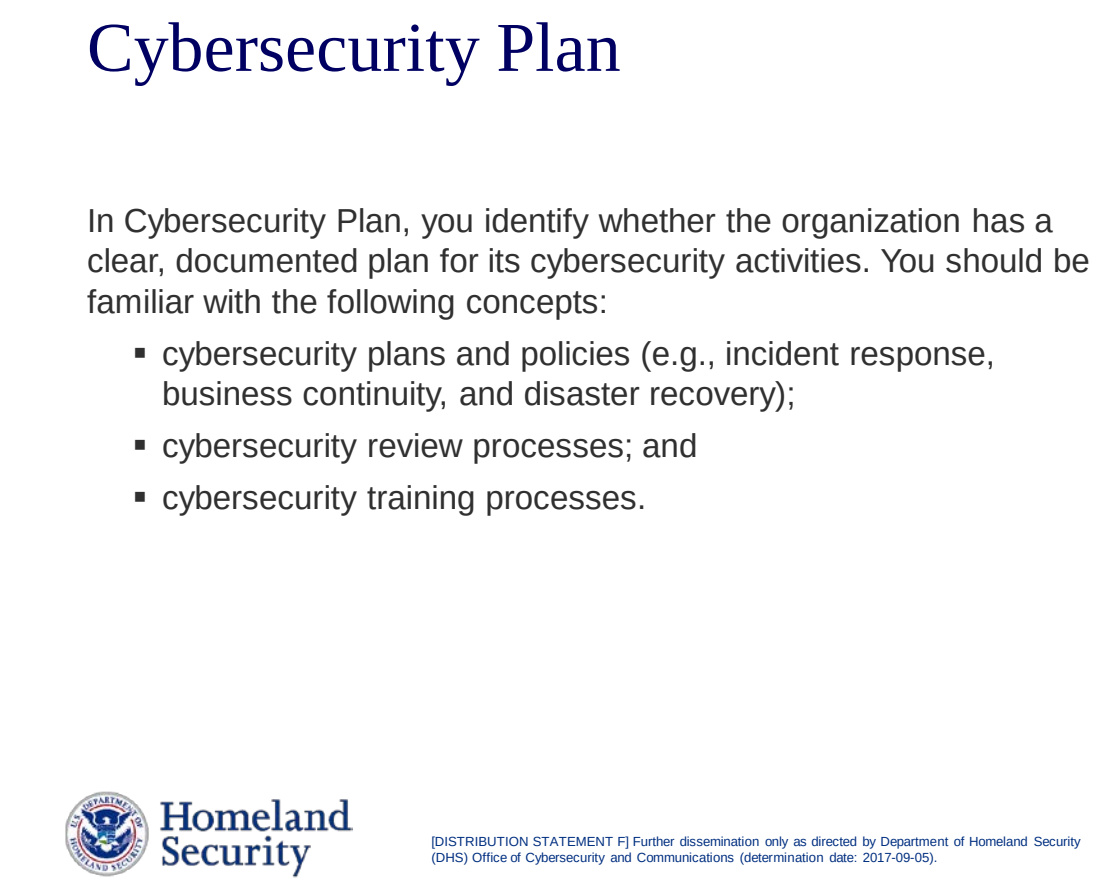
Assessment and Evaluation



**035 We then get into assessment and evaluation. So, you determine how the organization assesses cybersecurity practices such as management, operational, and technical of the critical service. So, we're going to be asking about established guidance and standards such as NIST, HITRUST, NERC CIP.

You want to be familiar with these different standards of practice that you can refer them to. You'll also want to be familiar with performing audits and vulnerability assessments. Who performs them, how to present the results? How are they done? The different types, you hit upon all those different aspects in that subdomain.

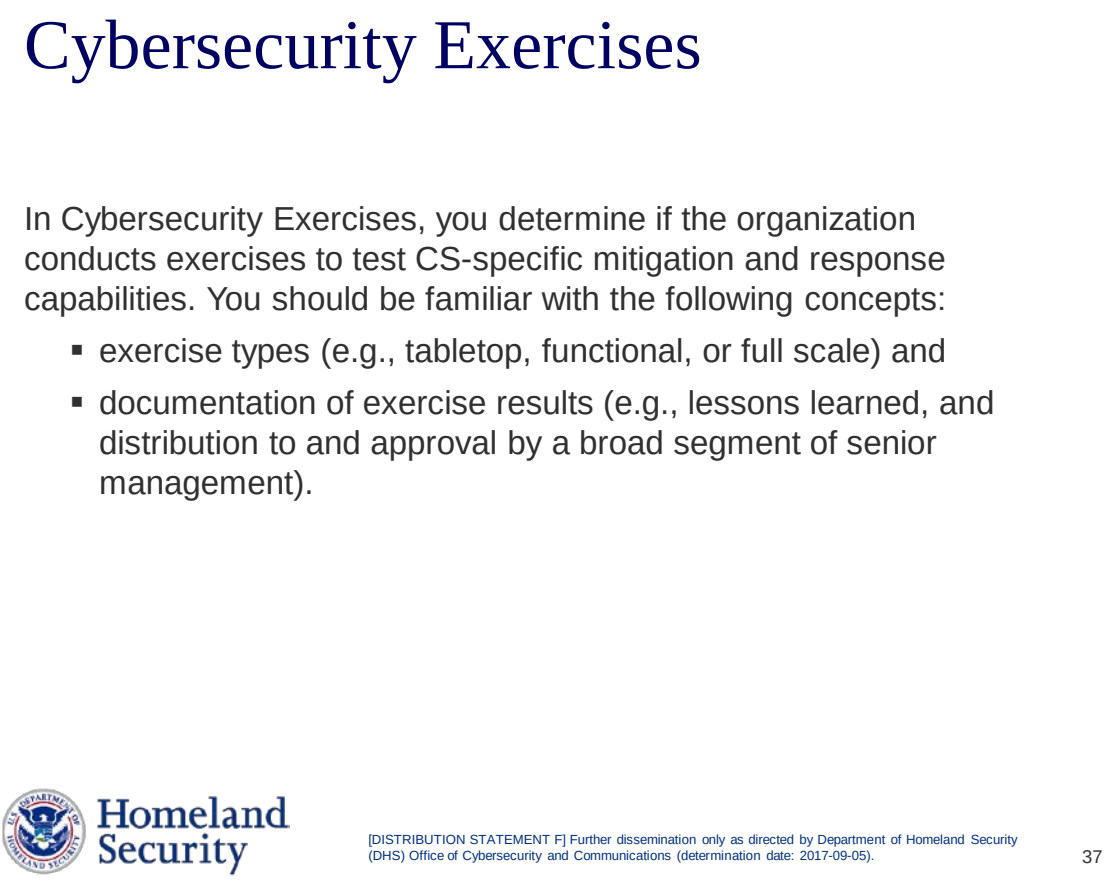
Cybersecurity Plan



**036 Then get into cybersecurity plan. So, does the organization have a clear documented plan for its cybersecurity activities? So, you should be familiar with what's contained within a cybersecurity plan and the different policies you would

have such as incident response, business continuity, cybersecurity review processes, the different training processes that are required.

Cybersecurity Exercises



**037 Cybersecurity exercises, so does the organization conduct exercises to test critical service specific mitigation and response capabilities? You should be responsible with different exercise types such as tabletop, full-scale, be able to explain here's when you would use a tabletop, here's a full-scale exercise, here's what that entails. And then also, documentation of exercise results, are you using

lessons learned after you perform and exercise?

Information Sharing

Information Sharing

In Information Sharing, you assess whether the organization conducts information-sharing activities with appropriate parties. You should be familiar with the following concepts:

- external information sharing,
- internal information sharing,
- cybersecurity incident reporting,
- vulnerability reporting,
- threat information sharing, and
- cybersecurity forums.

Homeland Security

**038 The next section of cybersecurity management is information sharing. So, does the organization conduct information sharing activities with appropriate parties? So, you should be familiar with the different external information sharing organizations that exist for that sector, internal information sharing practices, how you would do cybersecurity incident reporting, vulnerability management, knowledge of specific cybersecurity forums that you can point the organization to.

Cybersecurity Forces Domain

This domain determines the personnel assigned to maintain and operate the CS.

Cybersecurity Forces Domain	Checkbox	If Yes	Text Input	Notes	Total
Personnel	4	6		2	**12**
Cybersecurity Training	4	5		2	**11**
Total	**8**	**11**		**4**	**23**

**039 All right, the next main domain is cybersecurity forces. This is one of the smaller ones. But you're really going to be asking about personnel and how you train the personnel.

Personnel

In Personnel, you determine whether the organization's cybersecurity-related positions are formalized. You should be familiar with the following concepts:

- formalized cybersecurity positions (e.g., CSIRT staff, cybersecurity training official, security architect, system administrator);
- policies (e.g., for authorization or accountability); and
- background checks (e.g., employees and contractors).

**040 So, the first area is called personnel. And you determine whether the organization actually assigns cybersecurity related personnel. So, are they formalizing cybersecurity positions such as cyber incident response team staff? Do they have a cybersecurity training official? Do they have a security architect, system administrators? You want to-- you're going to talk about policies for authorization and accountability. So, how are you giving access and authorization to those cybersecurity related personnel? And then it also gets into background checks for employees and contractors if the organization is using third parties.

Cybersecurity Training

In Cybersecurity Training, you identify the type, frequency, and purpose of the organization's personnel training programs. You solicit information about the following:

- specific training for cybersecurity personnel (e.g., server administration, incident response, and risk management);
- basis of training (e.g., industry or government body of knowledge, and formal and informal in-house requirements); and
- delivery of training (e.g., video, web-based, classroom, and on-the-job training).

**041 Cybersecurity training attempts to identify the type, frequency, and purpose of the organization's personnel training programs. So, you're going to be asking about specific training for cybersecurity personnel such as server administration, incident response, risk management. You're going to be asking about basis of training. Is it industry or government body of knowledge? Is it formal, informal, in-house requirements, and then how you deliver that training, video, web-based, classroom, etc.?

Cybersecurity Controls Domain

This domain determines whether the organization has an effective baseline of security controls that govern the CS.

Cybersecurity Controls Domain	Checkbox	If Yes	Text Input	Notes	Total
Authentication and Authorization	9	7		2	**18**
Access Controls	5	3		4	**12**
Cybersecurity Measures	6	37		6	**49**
Information Protection	2	4		2	**8**
User Training	1	3		2	**6**
Defense Sophistication and Compensating Controls	1	1			**2**
Total	**24**	**55**		**16**	**95**

**042 Instructor: Are there any questions about the concepts and topics that you'll be asking about in previous domains? So, we'll continue this kind of high level walkthrough because it will set up the later parts of the course today, especially when we start to talk about some of the interaction between the domains and so forth. So, cybersecurity controls, this is another large domain. It's basically by the numbers here. And you can see kind of how that falls out. You're looking at ninety-five questions in this area.

Authentication and Authorization

In Authentication and Authorization, you determine how the organization's authentication and authorization controls are used on the CS. You should be familiar with the following concepts:

- authentication and authorization processes;
- identity proofing (e.g., risk based, controls based, best practices, and vendor based);
- authorization controls (e.g., access control, data loss prevention technology, management review, and rights suspension);
- administrator privilege controls (e.g., management approval, training requirements, and audits);
- authentication controls (e.g., password policies and multiple-factor authentication); and
- modifying, removing, and suspending accounts (e.g., due to change in employment status and change in roles).

Homeland Security

**043 So, one of the first actually subdomain, if you will, is authentication and authorization. The topics that you really need to be familiar with are authentication and authorization processes. So, it's important to understand the distinction. Identity proofing, there's different methods of doing that. Authorization controls, administrator privilege controls, these are all areas that will be asked about, or you will be asking about in the CIS. Modifying, removing, and suspending accounts, these are basic processes you will find typically in an organization, hopefully find.

Access Controls

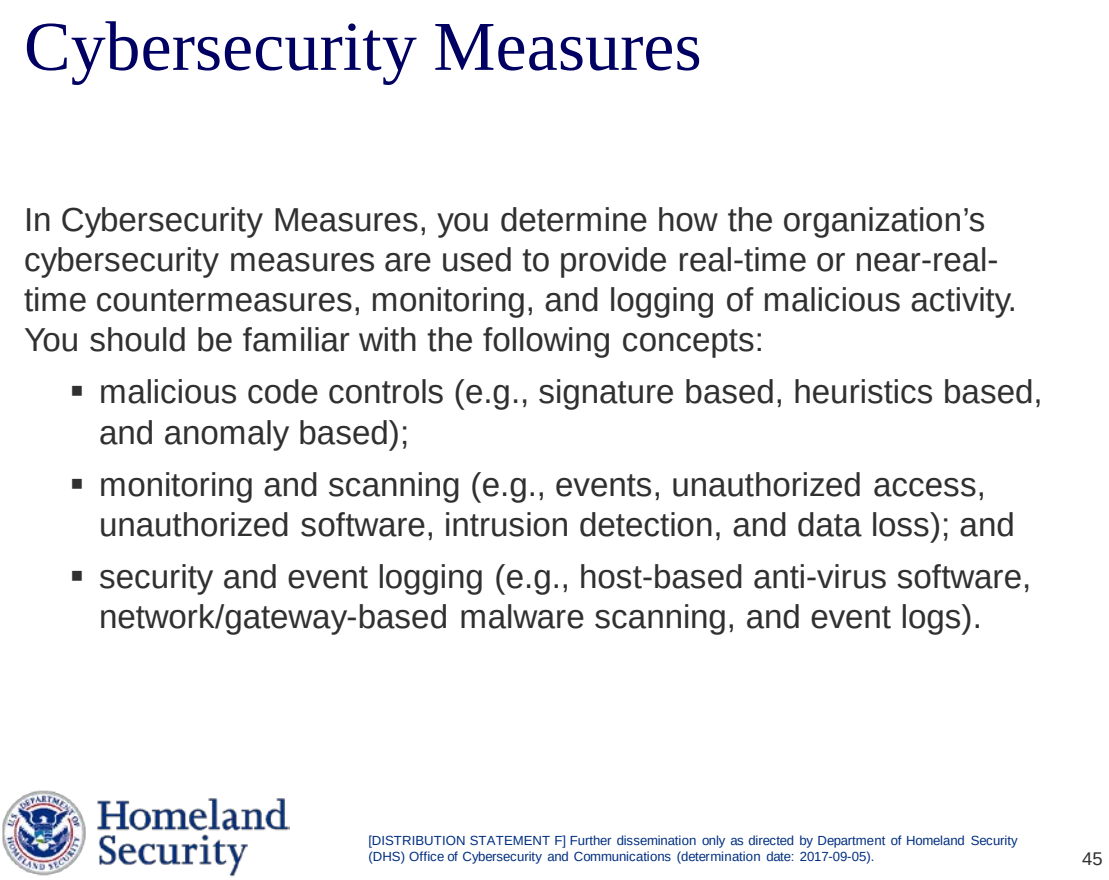
In Access Controls, you determine how the organization's access controls limit access paths to the CS. You should be familiar with the following concepts:

- access paths (e.g., boundary protections, access control devices, and preventing exploitation of access paths) and
- remote access controls (e.g., functional restrictions, remote client filtering, multiple authentication layers, multiple session restriction or monitoring, and session timeout).

**044 Access controls, what you're trying to do here is determine how the organization access controls limit access paths to the critical service. So, you're going to hear us repeat critical service a lot today because the questions are you're focusing on how that's done for the critical service, not the entire organization. So, an access path, your boundary protections, access control devices, preventing exploitation over those paths to portions of the critical service. Remote access controls, you're doing it for remote clients. It's a similar thing, multiple authentication layers potentially, multiple session restriction. Those are concepts you

should be familiar with as we go through this.

Cybersecurity Measures



**045 So, in cybersecurity measures, you're looking to determine how the organization's cybersecurity measures are used to provide real time or near real time counter measures, monitoring or logging of activity. Malicious code controls is a prominent topic in the CIS. Monitoring and scanning, and security and event logging are all aspects that you'll be asking questions about. So, you should be familiar with these concepts.

Information Protection

In Information Protection, you determine how the organization's information protection measures that used to protect sensitive information. You should be familiar with the following concepts:

- categorization of sensitive information (e.g., HIPAA, PII, and network diagrams);
- management of sensitive information (e.g., secure storage, controlling access, protective markings, and destruction procedures); and
- archive/backup of sensitive information (e.g., how often backups are performed, verified, and replicated).

**046 Information protection, how does the organization-- protection measures, how are they used? How effective are they? So, you're trying to determine those things. So, categorization of sensitive information is one aspect. The management of that information is another. And then the archive and backing up of that information is another aspect you're going to be asking questions about in this area.

User Training

In User Training, you determine when the organization trains users and gives them access to networks. You solicit information about the following:

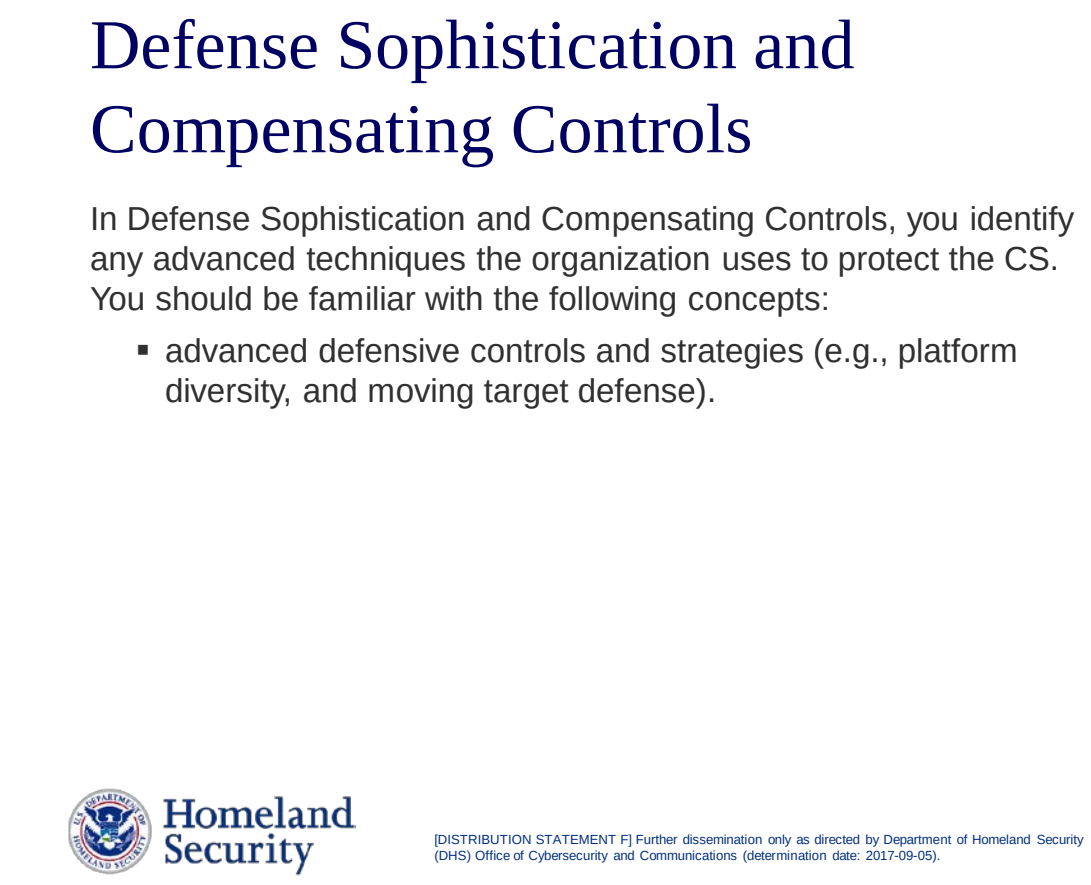
- user cybersecurity training and frequency (e.g., policies, roles and responsibilities, acceptable use, and password policies);
- method of training; and
- when training is provided (e.g., before a user obtains access or within 30 days of obtaining access).

**047 User training, so you're going to be looking to understand how the organization trains its users, both from a technical perspective-- so, for certain types of users, maybe administrators, security people, and so forth, and also from a general perspective for the end user as well. You'll want to understand the cybersecurity training and also the frequency of that training is what you're going to be trying to understand by asking the questions in the CIS.

When is the training provided? Again, that's also brought out. So, is somebody trained first before they're

allowed access to the network? Does it happen within thirty days? Does it happen at all? Those are aspects that are asked about in the CIS.

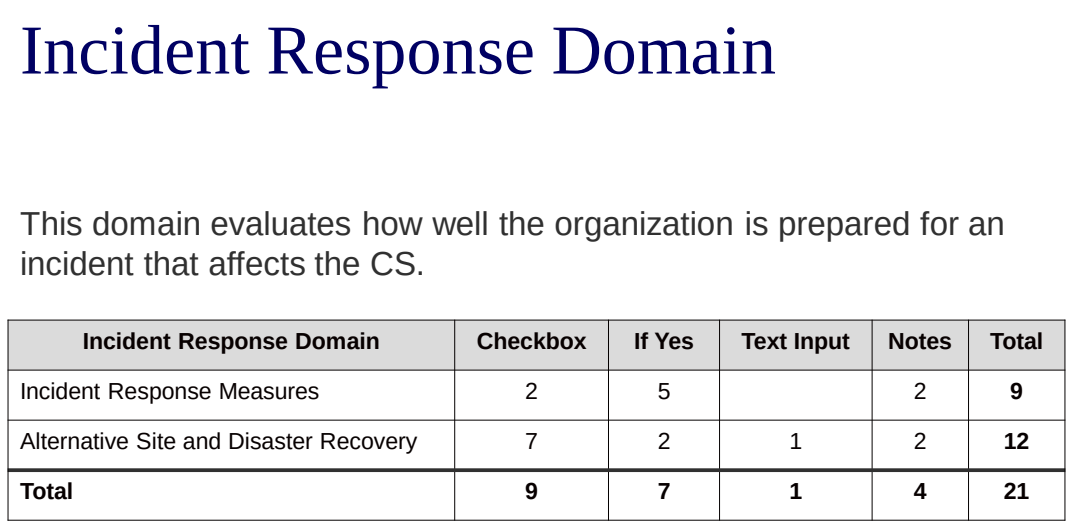
Defense Sophistication and Compensating Controls



**048 So, another subdomain, if you will, is defense sophistication and compensating controls. So, in this area, you're going to try to identify advanced techniques that an organization may be using that maybe you're not seeing everywhere else. So, those advanced controls and strategies is what you're really trying to define here. So, this does not mean best practice. And in our last section, you're going to see us

indicate what common best practices that the CIS is trying to bring out. But this is something that's unique that maybe somebody is not-- that not all people are doing. And we'll get into more of this in a later section.

Incident Response Domain



Incident Response Domain	Checkbox	If Yes	Text Input	Notes	Total
Incident Response Measures	2	5		2	**9**
Alternative Site and Disaster Recovery	7	2	1	2	**12**
Total	**9**	**7**	**1**	**4**	**21**

**049 So, the incident response domain. You can see this is much smaller. By this point, you've probably covered a majority of the CIS as most of you are aware. This is focusing in on two areas, incident response measures and alternative site and disaster recovery aspects.

Incident Response Measures

In Incident Response Measures, you identify the organization's documented plans and procedures. You solicit information about the following:

- incident response plans (e.g., plans containing documented procedures and roles);
- incident response procedures (e.g., procedures for network containment, malware containment, and denial-of-service attack response);
- testing response procedures (e.g., frequency and test methods);
- reviews of cyber events in the context of the CS; and
- incident response contracts with external entities (e.g., industry response networks).

**050 So, incident response measures, you're trying identify-- you identify the organization's documented plans and procedures. What do they actually have in place? You're trying to solicit the following types of information, incident response plans. Are they documented? Do they have them? What are their procedures? How do they test? Review of cyber events, like what are they doing there? So, those are the type of aspects you're going be trying to determine.

Alternate Site and Disaster Recovery

In Alternate Site and Disaster Recovery, you determine the organization's disaster-recovery capabilities. You solicit answers for the following:

- impacts of a system outage or loss (e.g., percentage of normal business functions lost or degraded, and length of time the organization is affected);
- business continuity plans and alternate locations (e.g., alternative site characterization, percent of the main facility's capacity, and time needed for a move);
- restoration and recovery (e.g., time to recover, service level agreements, and continuity of operation agreements); and
- disaster recovery testing (e.g., how often and what types).

**051 Alternate site and disaster recovery, you're determining the organization's capabilities in these areas. You're trying to solicit answers to the following types of topics, impacts of system outages or losses. What is the impact from that? What are their business continuity plans, if they have any? What are restoration and recovery? How is that being accounted for? And what kind of testing are they doing in this area? Testing is probably, in most organizations, the only way they're going to really understand if these things are working. That's really the only way you're going to know for sure.

Dependencies Domain

This domain identifies the CS's dependence on data generated or stored by a system and evaluates the organization's mitigating controls and procedures.

Dependencies Domain	Checkbox	If Yes	Text Input	Notes	Total
Data at Rest	1	5		2	**8**
Data in Motion	2	18		2	**22**
Data in Process	1	8		2	**11**
Endpoint Systems	1	5		2	**8**
Total	**5**	**36**		**8**	**49**

**052 So, the next domain in the CIS is the dependencies domain. What you're doing is identifying dependence on data generated or stored by a system and evaluates the organization's mitigating controls and procedures. That's what you're trying to do. So, there's four different subdomains here, data at rest, what's in motion, data in process, and endpoint systems.

Data at Rest

In Data at Rest, you examine the organization's requirements for protecting stored data in the CS. You solicit information about the following:

- data storage requirements (e.g., dependency on a storage area network [SAN] or server, dependency on a human machine interface [HMI], etc.);
- length of time before the CS is severely affected by a loss;
- percentage of normal cyber functions lost or degraded; and
- failover and restoration procedures (e.g., backup or alternatives, and length of time needed to fully resume operations after a system restoration).

**053 So, for data at rest, you're examining the organization's requirements for protecting stored data. What's on disk? What's on tape? What's on a particular system? So, what are data storage requirements? What's the length of time before a critical service is severely impacted if you lose that data, or if it's not available? Percentage of normal function lost if that's not available, and what are fail over and restoration procedures? Those are the areas you're going to focus on here.

Data in Motion

In Data in Motion, you examine dependencies on the organization's communication paths, both internal and external. You solicit information about the following:

- external communications (e.g., public-facing systems and VPN-reliant system);
- internal communications (e.g., does not communicate across the Internet);
- length of time before the CS is severely affected by a loss;
- percentage of normal cyber functions lost or degraded; and
- restoration procedures (e.g., contingency/business continuity plan, backup mode of communication, and length of time needed to fully resume operations).

**054 Data in motion, it's what you expect, the data that's traveling over the wire, basically. You're going to examine dependencies on the organization's communications path. What happens if those paths aren't available, both internal and external? So, external communications-- internal communications, as we've said are prominent. And again, a common set of other features here like length of time before the service is impacted if those aren't available, percentage of normal function that's lost. You're narrowing down those same aspects depending on what is affecting the service, and in this case, data in motion.

Data in Process

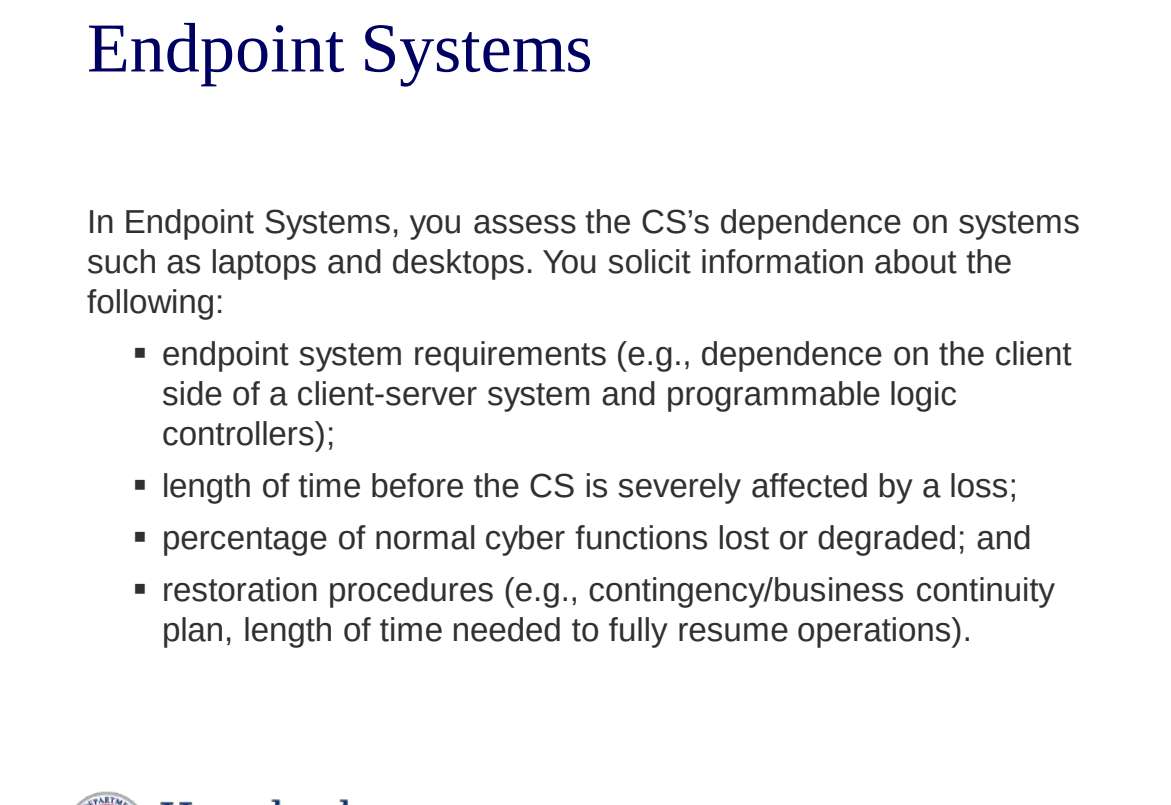
In Data in Process, you examine the organization's dependence on data-processing services, such as cloud providers. You solicit information about the following:

- data processing requirements (e.g., mainframes, server farms, cloud providers);
- length of time before the CS is severely affected by a loss;
- percentage of normal cyber functions lost or degraded;
- restoration procedures (e.g., contingency/business continuity plan, length of time needed to fully resume operations); and
- external dependencies (e.g., external data service providers such as a geographical information system [GIS], and dependency monitoring).

**055 So, data in process, so you're going to examine the organization's dependence on data processing services, maybe a cloud provider as an example. You're going to solicit information about the following, data processing requirements. As you see, mainframe, server farm, cloud providers, the type of things you'll be asking about. The length of time before the service is severely affected. So, again, we're going into those common themes. So, if some of the data processing capability is affected, how does that affect the service? What percentage of normal function is lost? What are the restoration procedures? It's a

common set of themes for all these different aspects is what you're seeing in this domain.

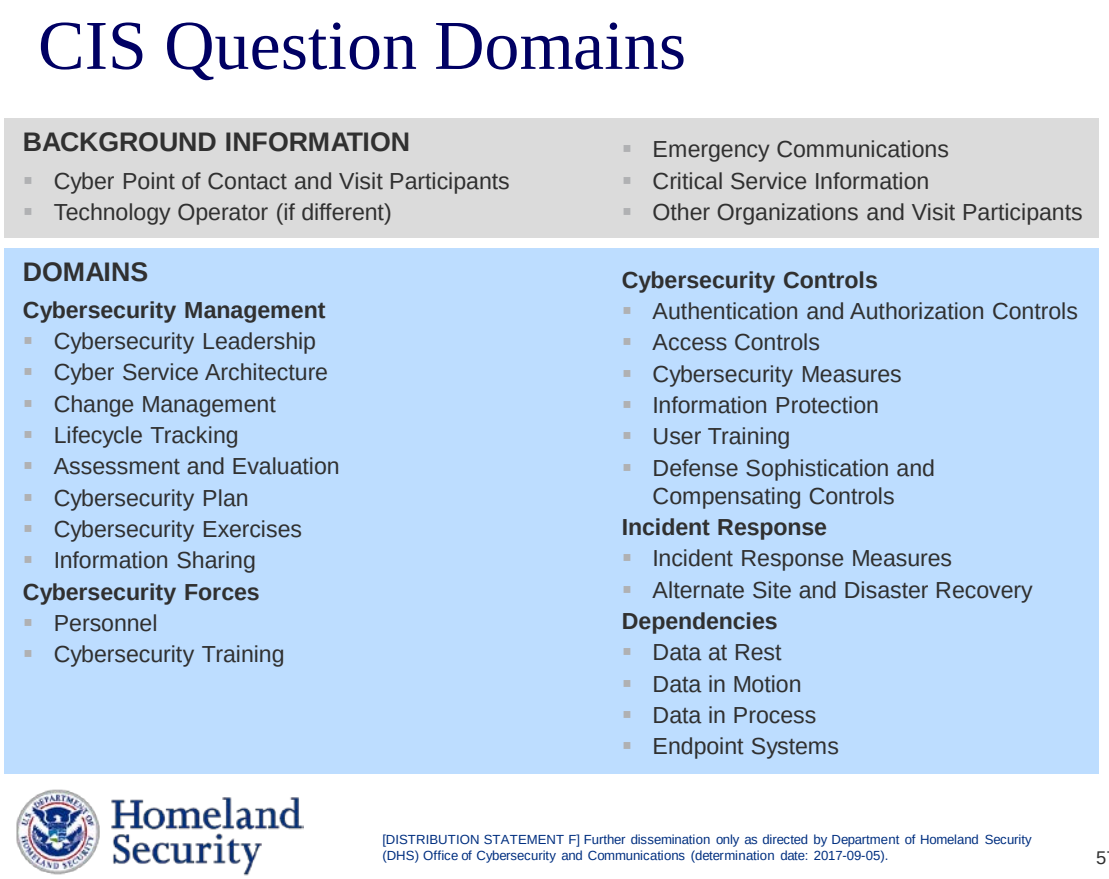
Endpoint Systems



**056 End point systems, so you're going to assess the critical service dependence on end point systems. So, if there's somebody on a laptop or desktop that is key to that service and is not receiving the data they need, that's where this kind of comes into play. What are the end point system requirements? Now, you're getting to, again, the same set of common attributes that we're trying to evaluate on how that end point system really affects the service, the

length of time before it's severely affected, the percentage of normal cyber functions lost, and what are the restoration procedures for that part of the service.

So, the CIS breaks it up into those areas, but you're trying to solicit that kind of view at all those areas. So, you can now piece together how that service is going to be affected by any of those data aspects. So, from a higher view of the CIS, which you're not kind of getting as you're asking all the questions, you can kind of see how all this starts to tie together.



**057 So, again, that's kind of the walkthrough of the domains. This is meant just to refresh you on all the domains there are that we just walked through. You can see the main subdomains listed there.

Administering the CIS: Objectives Summary

In this section, you learned

- the types of questions in the CIS,
- the concept of least common denominator, and
- the intent of each CIS domain.

**058 So, in summary, we went through the types of questions that there are, how to answer some of those. We went through the concept of least common denominator, which is important because that is how you have to approach answering the questions in the CIS. You need to take that approach. That's what's being expected. And we just gave a high level overview of what's contained in each of the domains of the CIS. Any questions on what we saw in that section?

Introduction

Table of Contents

Managing the Engagement

September 2017

Homeland Security

**001 Instructor: All right, this section is called Managing the Engagement.

**002 [Notice]

Managing the Engagement: Objectives

After completing this section, you will be able to

- learn the phases of the CIS engagement and management process,
- apply best practices and tips to manage the engagement, and
- use the dashboard to benefit the organization.

**004 So the objectives of Managing the Engagement consist of: You want to learn the phases of the CIS engagement and management process; apply best practices and tips to manage the engagement; and use the dashboard to benefit the organization.

Managing the Engagement: Topics

CIS Process

- Receiving the Request
- Conducting the Pre-Survey Call
- Conducting the Survey
- Processing the Survey
- Providing the Dashboard to the Organization

CIS Dashboard

**005 So there's two distinct sections to this area. We're going to talk about the CIS process and get more detail into all those phases listed, as well as talk about the CIS dashboard.

CIS Process

Table of Contents

CIS Process

Cyber Infrastructure Survey (CIS) Training Course

**006 So the process.

CIS Process: Overview

There are five main phases to the CIS process:

1. An organization requests a CIS (hereafter called survey).
2. The assessor calls the organization to collect information and schedule the assessment.
3. The assessor conducts the survey on-site, ensuring all questions are answered.
4. The assessor processes the survey and prepares the dashboard.
5. In a debrief, the assessor provides the dashboard to the organization and discusses relevant DHS capabilities.

Homeland Security

**007 What you see here is a high-level overview of the CIS process, which consists of five main phases: You receive a request for a CIS; you conduct a pre-survey call; you can conduct the survey; you then process the survey; and then you end it with providing the dashboard to the organization. We're going to go into detail of each activity for those phases.

Receive a CIS Request

Organizations in the Critical Infrastructure and Key Resources (CIKR) sectors and state, local, tribal, and territorial (SLTT) governments in the United States (and its territories) can request a CIS.

Tip

The CIS process is voluntary; participation is not federally mandated.

Homeland Security

**008 So, who can request a CIS assessment? Pretty much any organization in critical infrastructure and key resource sectors and state, local, tribal, and territorial governments in the United States can request a CIS. So if they're in the 16 sectors that we listed or state, local, territorial governments and you can relate their mission to critical infrastructure, they can request a CIS. Just remember the CIS is a voluntary process. The organizations are requesting it, and the participation is not federally mandated.

Conduct the Pre-Survey Call

As the assessor, you are responsible to make a pre-survey call **before the on-site survey is conducted**. During the call, you do the following:

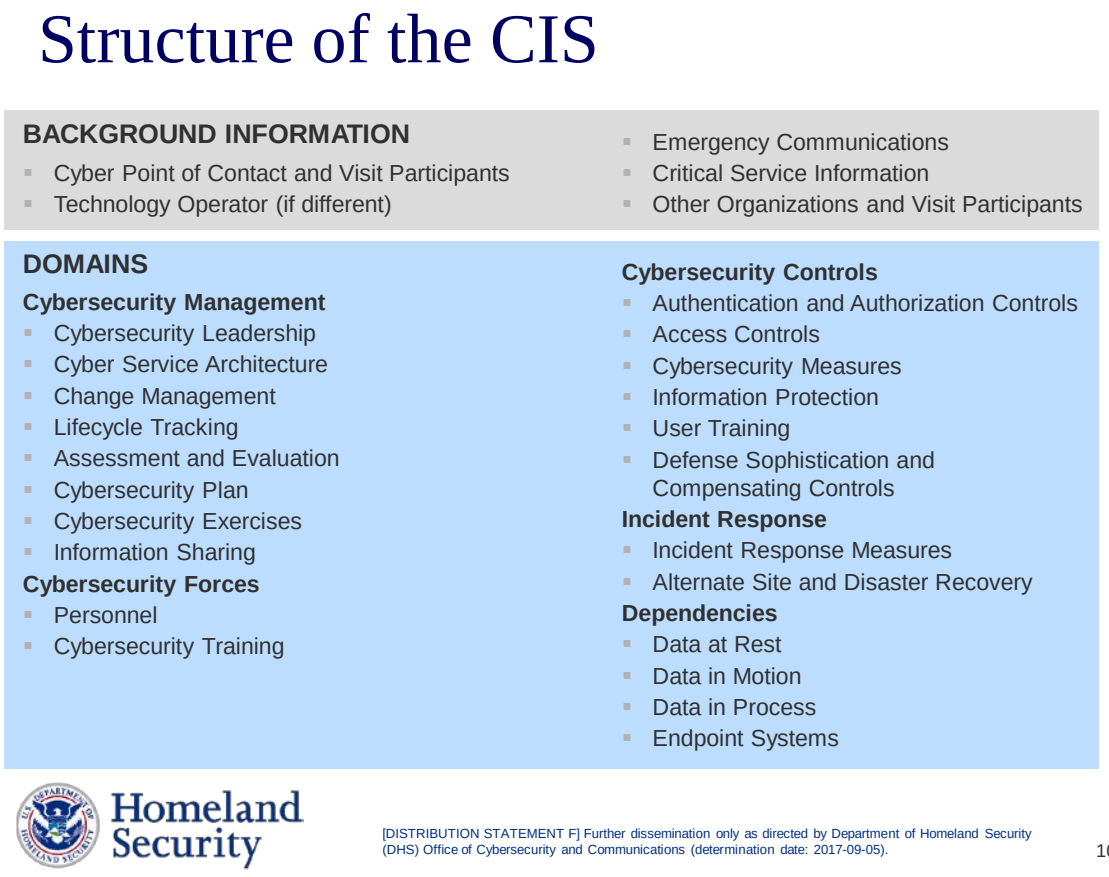
- Provide an overview of the CIS domains.
- Review the Protected Critical Infrastructure Information (PCII) Program.
- request the signed PCII Express and Certification Form from the organization.
- Discuss who should participate in the CIS process.
- Complete the Demographic Questionnaire.
- Complete the Background Domain portion of the survey.
- Determine the scope of the CS.
- Schedule the survey.

Homeland Security

**009 So after you receive the request, you're going to want to schedule the pre-survey call. This call happens before you get onsite. A lot of the stuff you should have gathered before you get onsite to help facilitate the day of, but it's going to-- when you schedule the call you're going to want to provide an overview of the CIS domains; you're going to want to review what protected critical infrastructure information program is, the PCII program; you want to request the signed PCI Express and Certification form. During this call you're going to discuss who should participate in the process whenever you're onsite. You

want to complete as much as the demographic questionnaire as you can during the pre-survey call. You also want to complete as much of the background domain portion of the survey as well-- so critical service description, if you can scope it. Determine the scope of the critical service on this call. This more information you can gather from the call, that'll assist you on the day of and actually ensuring that you have the right people in the room when you arrive onsite. And then finally you want to schedule the survey.

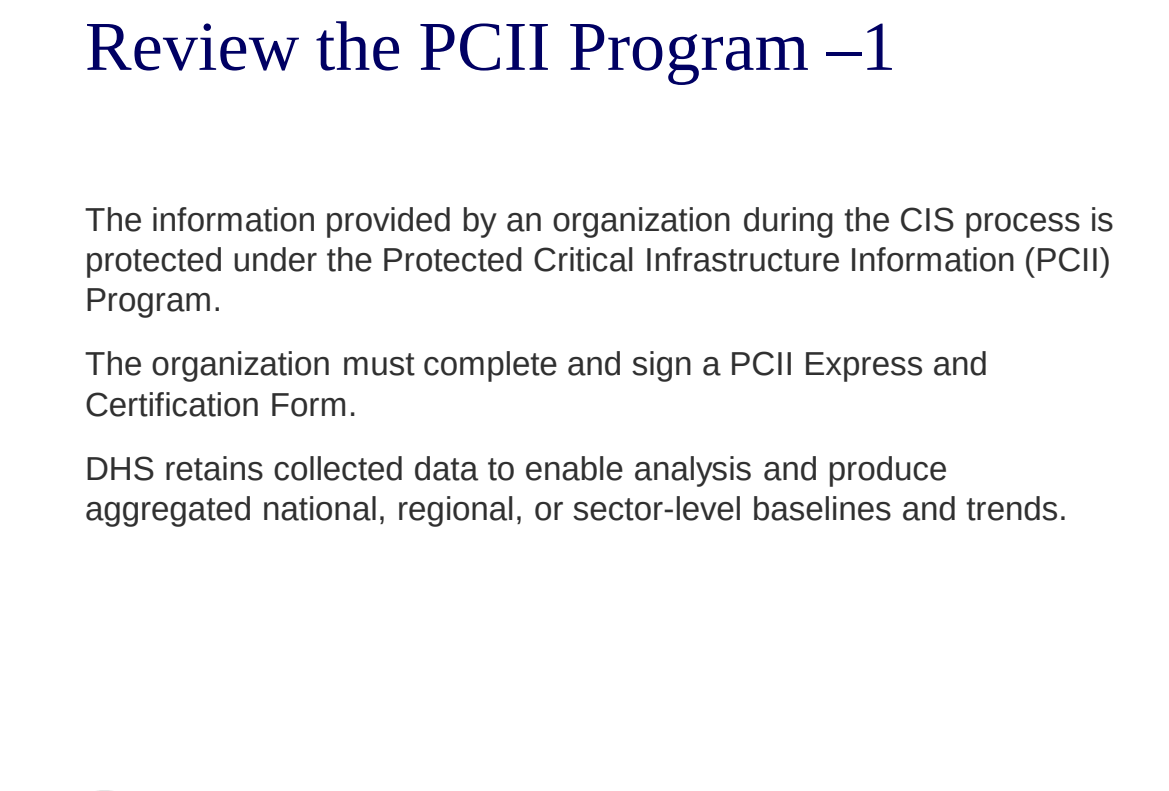
Structure of the CIS



**010 So again, high-level, just to

drill it in, five domains, background domain.

Review the PCII Program –1



**011 So part of the call, you're going to want to review the PCII program with the organization. So let them know that the information they provide to you guys is protected under the PCII program. To enable them to receive that protection, you have to complete-- or they have to complete-- the PCII Express and Certification form, and you want to explain that you retain collected data to enable analysis so you can produce the aggregate-level graphs to kind of see where they fit in within

the different sectors and organizations. Question?

Student: The PCII Express and Certification form, is that a form that we send to them, or is it something that we present to them once we get onsite and we're about to start?

Instructor: From what I know, and you guys may be able to answer more appropriately, it's an in-paper form that you email to them.

Instructor: You just email it.

Instructor: But we've done both. So I always carry an extra copy with me if I don't have it and it's scheduled, and then when I get there and I say, "You got to sign this now."

Student: Will it let you proceed through the workflow if you don't check off the questions that say you have the form?

Instructor: We can talk about that offline.

Student: I haven't had that come up. That's why I ask.

Instructor: So it's yes and yes.

Instructor: So the expectation is that this discussion would happen beforehand. You're trying to get it beforehand. Reality, as he's suggesting, is sometimes that doesn't happen. But the expectation is to try to get it beforehand.

Instructor: It's easier if you can get it done first.

Student: Yeah. You don't want to walk in there and--

Instructor: Every situation tends to be a little different.

Instructor: See, I actually even do that before I do pretty much anything else, because the way it was explained to me, once you start discussing the assessment, including defining the critical service, that itself is PCII. So you should have that signed before you even have that conversation.

Instructor: Yes.

Instructor: Well, that would be nice. However, you send it in, and it doesn't get validated; until headquarters validates it and sends it back--

Instructor: I don't care about that. I'm just making sure that they sign something.

Review the PCII Program –2

PCII program protection means that

- DHS cannot be compelled to publicly disclose PCII.
- DHS employees and contractors who access PCII must be certified as PCII Authorized Users and may access PCII only according to DHS safeguarding and handling requirements.
- PCII cannot be used for regulatory purposes.

For more information about PCII, visit the DHS website at https://www.dhs.gov/pcii-program.

**012 Instructor: Yeah, you're correct. The expectation is to do it up front, as best you can.

Instructor: So more information on PCII protection means. You cannot publicly disclose the PCII. Employees and contractors who access the information are trained on how to handle it, and the PCII can't be used for regulatory purposes. If you want more information on the program, dhs.gov/pcii-program.

Obtain the PCII Express and Certification Form

The organization must complete and sign the PCII Express and Certification Form and submit it to you as the assessor. This form contains the following components:

- **Certification Statement** – Authorizes named individuals to submit information on behalf of the organization
- **Express Statement** – Confirms that submission of the information is voluntary
- **Access Disclosure** – Authorizes applicable individuals to access the submitted information based on their need to know
- **Contact Information** – Provides contact information for the submitter and alternate submitter

Tip

Get the signed PCII Express and Certification Form before going on-site.

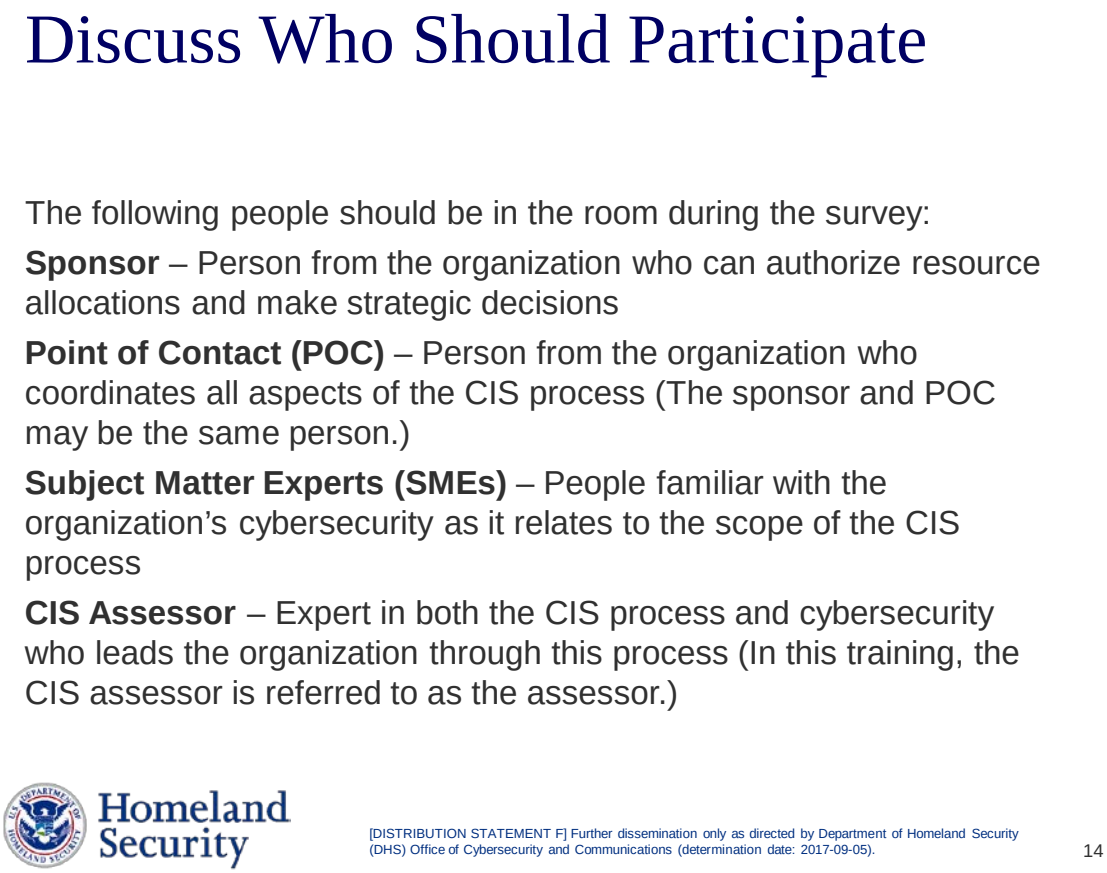
Homeland Security

13

**013 So what are the different sections of the PCII Express and Certification form? You have the certification statement, which authorizes the named individuals of the organization to submit information on behalf of that organization. You have the express statement, confirms the submission of the information is voluntary. Access disclosure-- it authorizes applicable individuals to access the submitted information based on their need to know. And contact information, so provides the contact information for the submitter, and there's a spot for alternate submitter as well. So as we've stated, best

practice is to get this signed form before going onsite whenever possible.

Discuss Who Should Participate



**014 Also during this call you want to discuss who should participate in the survey. So typically we have a sponsor, so that's the person from the organization who can authorize resource allocations and make strategic decisions. You have a point of contact, so the person from the organization who coordinates all aspects of the CIS process. A lot of times the sponsor and the point of contact are the same. Any subject matter experts from the organization,

so people familiar with the organization, cybersecurity, as it relates to the critical service and the CIS process, and then you as the CIS assessor, expert in both CIS process and cybersecurity who leads the organization through the process. So I'll just be referring to that individual as the assessor for the rest of this section. Any questions?

Complete the Demographic Questionnaire –1

Complete the Demographic Questionnaire –1

Before accessing and starting the survey, you, as the assessor, must complete the Demographic Questionnaire during Phase B of the CIS process.

During the pre-survey call, you complete the Demographic Questionnaire on the portal.

Collecting this information supports data analysis.

Tip

In the CIS, some information is collected in Phase A.

Homeland Security

15

**015 Okay. During this call you want to attempt to complete as much of the demographic information as you can. So for the way that the portal works, before you can even access the survey, you have to

submit-- or you have to collect the information from Phase B demographics. So you want to complete the information found in Phase B during the pre-survey call, and then also the background domain of the CIS, there's a lot of overlap between the background information and the demographic information. So you'll find also while you're in Phase A of the workflow, you're also collecting demographic information, but the idea being you want to collect as much of this as you can on this call.

Student: Sorry to go back to Slide 14.

Discuss Who Should Participate

The following people should be in the room during the survey:

Sponsor – Person from the organization who can authorize resource allocations and make strategic decisions

Point of Contact (POC) – Person from the organization who coordinates all aspects of the CIS process (The sponsor and POC may be the same person.)

Subject Matter Experts (SMEs) – People familiar with the organization's cybersecurity as it relates to the scope of the CIS process

CIS Assessor – Expert in both the CIS process and cybersecurity who leads the organization through this process (In this training, the CIS assessor is referred to as the assessor.)

**014 So compared to the CRR, which might have a larger audience or group who participates, what's the purpose for having a smaller group for this? Is it because the CIS is a lightweight assessment?

Instructor: It was designed that way. That's correct. It was designed to require a smaller group and to be done in less time, and it's very targeted to control-based assessment. So that was part of the structure from the beginning.

Complete the Demographic Questionnaire –2

As the assessor, you must collect the following demographic information:

- number of employees;
- annual funding;
- number of customers served by the CS;
- critical infrastructure sectors that support the organization;
- what, if any, standards or bodies of practice are being used;
- what, if any, regulations govern the organization; and
- if the organization shares cybersecurity data with others.

Tip

There might be overlap between the information you collect for the Background Domain of the survey and the Demographic Questionnaire.

Homeland Security

16

**016 Instructor: So some of the information you're going to be capturing with the demographic questionnaire is number of employees in the organization and the business unit, annual funding, the number of customer service by the critical service, the critical infrastructure that support the infrastructure sectors that support the organization-- what standards and bodies of practices are you using? The idea being here is as we get more assessments and we can get this fine-level detail, we can start to make some observations and kind of bin appropriate organizations for them to get a sense of how well

they're actually doing compared to their peers. So again, there's some overlap between the background domain and the demographic questionnaire.

Student: One of the questions that I've been asked, when you talk about numbers of customers, like say a hospital-- a hospital might have 700 beds and service, I don't know, 150 people a day in their ER. So that number of customers, is it on the annual basis? Is it a snapshot? Like, "Right now, how many people do you have under patient care in your hospital?" Or is it a total number? Like a water treatment facility might say, "We have right now 40 thousand customers." So that's easy. But where there's other industries or sectors that have shifting numbers depending on their--

Instructor: Yeah, so they may give you a number based on, "In a year we, on average, see X number of patients," right? I would probably take the way they do it.

Student: That's what I did, but I just wanted to make sure I was doing it right.

Instructor: Yeah, but I would also note that where you could. Like you could phrase it that way. If that's how they're measuring themselves, I would probably use that method.

Student: So it's more like how they measure themselves is what we're capturing? That's a good way to look at it?

Instructor: I think it is, and at CERT-- the example you gave is a good one, right? So water, it's a set number, like they know--

Student: Well, it is and it isn't. They have 40 thousand households, but how many persons per household?

Student: No, from their standpoint, they would look at it as who pays the bill.

Instructor: Correct.

Instructor: Correct. So you're probably going to end up using that number. That's what they're going to-- it's how they're measuring themselves once again, right? And again, in a hospital--

Student: In a hospital, are you looking at beds? Number of beds versus number of patients?

Instructor: They may tell you that on an average year they do this many-- they have this many patients basically, right?

Student: Yeah, it really is just-- it's demographic background information. It's not anything that's going to affect the assessment one way or the other. Perhaps maybe in the number of-- how they get gauged against--

Instructor: Like the number of beds is one thing, but those beds are typically filled by many different people throughout the year, right?

Student: Yeah, you could have the same bed, three different patients in one day.

Instructor: Exactly. So it's probably a better number to use what they are doing, "On average for a yearly basis, we support this many patients."

Student: For annual funding, are you looking at overall funding for the organization or are you looking at specific tools?

Instructor: Oh, so there are specific questions I believe that kind of get to some of that.

Student: Got it.

Instructor: Yeah, I think it's at the organization level and then there's also a lower level organization, like business unit, department as well.

Student: Like operating cost.

Instructor: Yeah.

Student: A percentage.

Instructor: Yeah. So in both areas of the demographics, you may see funding for an overall level, because you're trying to understand if it's an HP or an IBM versus a local kind of provider, and maybe somebody in that middle tier or lower. But then you also see questions in regards to maybe at a department level, what's available, or even potentially for the service itself.

Student: Just from a feedback perspective, I've yet to see anybody spend more than 10 percent on their cybersecurity funding, because it was one to ten and all that, and so there's hardly anyone that's spending more than 10 percent on their cyber. So that question really falls off and there's there.

Instructor: But those are some of the insights that we're trying to develop, along with being able to group like for like and other aspects, right?

Student: I'm sure you're getting that data and it's just one big-- everybody's 1 to 10 percent.

Instructor: Yeah, we are-- if you think about it, we only recently started to collect demographic data for the other assessments. So starting to look at that will be interesting, I think.

Instructor: Any other questions on demographics?

Complete the Background Domain in the Survey

As the assessor, you must complete the Background Domain of the survey by collecting information such as

- personnel information,
- CS descriptions,
- names of IT/ICS systems that support the CS,
- budget information, and
- general descriptions of networks, services, applications, connections, etc.

Tip

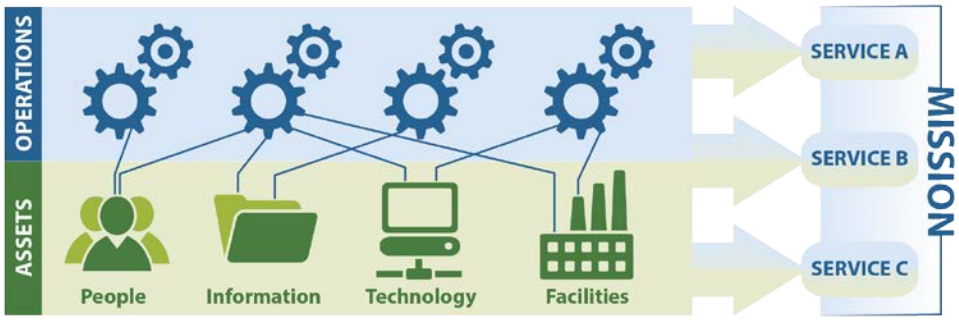
You may have to make multiple calls to gather all the information.

Homeland Security

17

**017 So again, more of the same here. The background and demographics overlap a lot, but in the background domain it's asking personnel information, asking for critical service descriptions; it's asking for the names of the IT-ICS systems that support the critical service. Again, budget information. You may have to make multiple calls or just be aware when you get onsite, "Hey, we still have some of these open items for before you start the service." But you should have this information collected before you start the survey.

Determine the Scope of the CS



An organization uses its **assets** to perform **productive activities** that enable it to provide operational **services** and accomplish its **mission**.

Best Practice

Throughout the survey, emphasize the selected CS.

Homeland Security

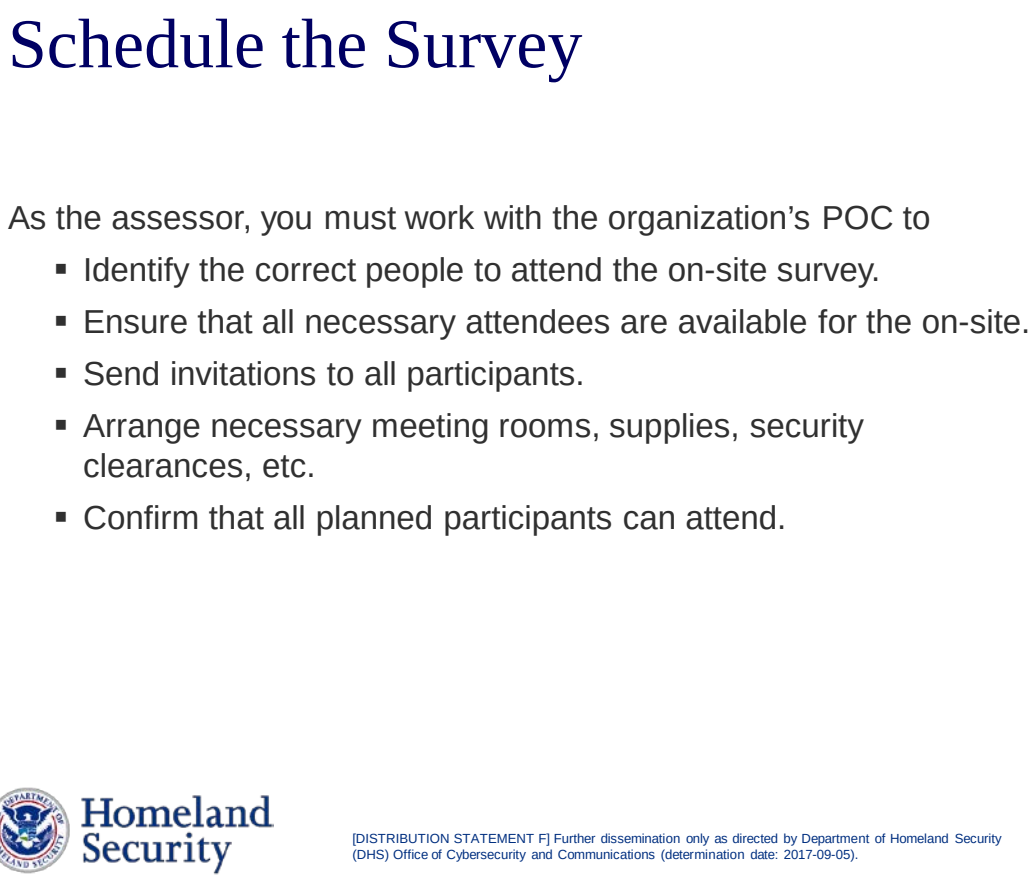
18

**018 Also during this call you want to determine the scope of the critical service. So as we explained the critical service methodology earlier, you really want to come out of this call with an idea of what you're going to be assessing that day that you show up onsite, and then a best practice is once you have this, emphasize that critical service throughout the day as you're asking these different practice-type questions.

Instructor: Right, and as the previous slide said, it may take more than one call to really tamp this down, because they may need to go

and think about-- their understanding after the discussion is probably going to be different than what they started with. So they may need to go and think about that, and it might be better-- like if you get the sense that an additional call is needed, it might be better to schedule that.

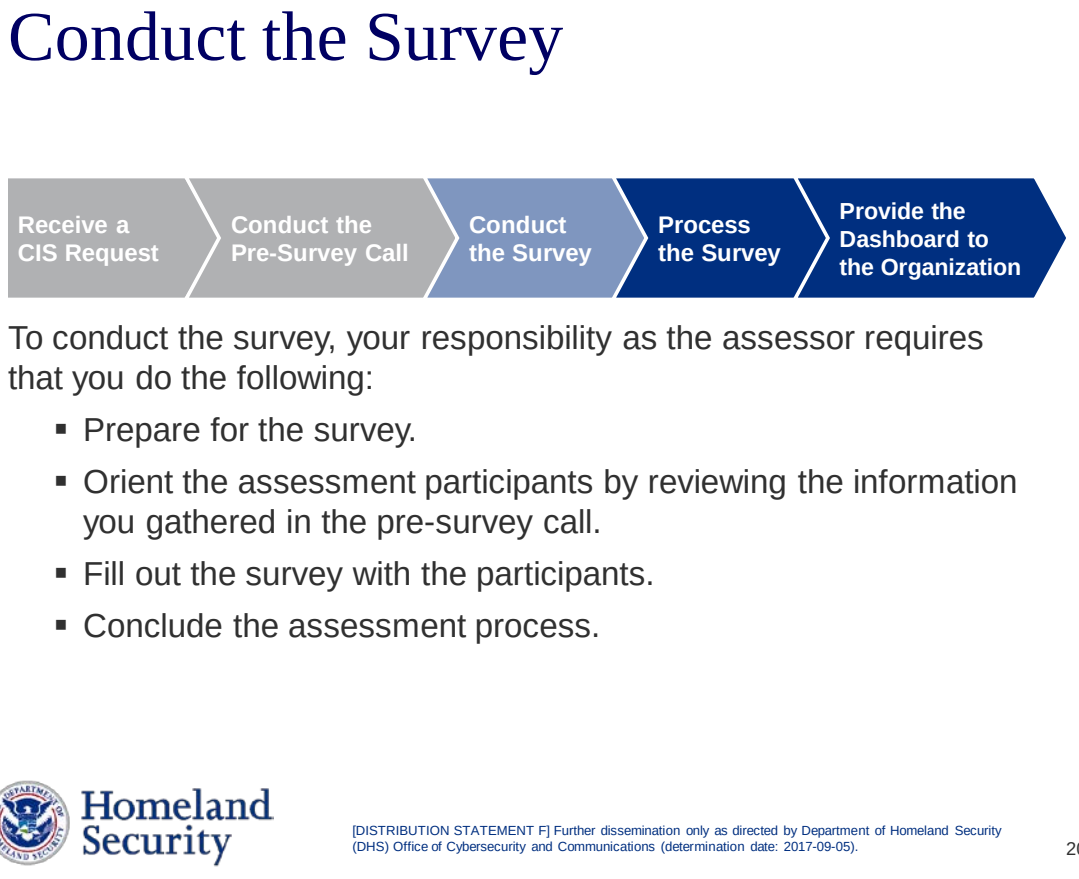
Schedule the Survey



**019 Instructor: And then finally, you want to schedule the survey. So identify the correct people that need to attend the onsite portion. You want to ensure that all the necessary attendees are available for the onsite. You're going to send invitations to all the participants. The

point of contact should arrange the necessary meeting room, supplies, security clearances, etcetera, and then confirm that all plan participants can attend.

Conduct the Survey



**020 Now we're at Conduct the Survey. So this is the day that you show up onsite. So we're going to prepare for the survey, orientate the assessment participants by reviewing information, fill out the survey with the participants, and conclude the assessment process.

Prepare for the Survey: Your Approach

Before you arrive on-site, prepare by doing the following:

- Study each domain so that you understand it thoroughly.
- Imagine the types of questions you might need to ask to
  - understand the organization's CS and
  - elicit the type and amount of information required to adequately answer the survey questions.
- Learn more about the organization and its industry.
- Practice meeting-management skills that help participants remain engaged and contribute to a successful event.

Tip

Bring a paper copy of the survey in case there are any technical issues that prevent you from displaying content.

Homeland Security

**021 All right, Prepare for the Survey. What should your approach be? So as I stated earlier, you're going to be going through the survey asking questions, and then right away the spotlight is going to be on you and you're going to have to explain what these concepts are. So be familiar with each domain and understand what's coming and even come up with some examples that you've had based on previous work experience-- different best practices you've seen in the organizations that you've assessed already. But be ready to discuss the different domain concepts.

Imagine the type of questions you might need to ask to understand the organization's critical service and elicit the type and amount of information required. So one of the things I like to do is when we get onsite, we may have a critical service identified, but I just ask them, "Can you review it? Can you tell me all the different connection points?" If they want to draw it out to get kind of a high-level diagram, I like to do that sometimes. But what type of software are they using? Just anything that can help me focus my questions throughout the day.

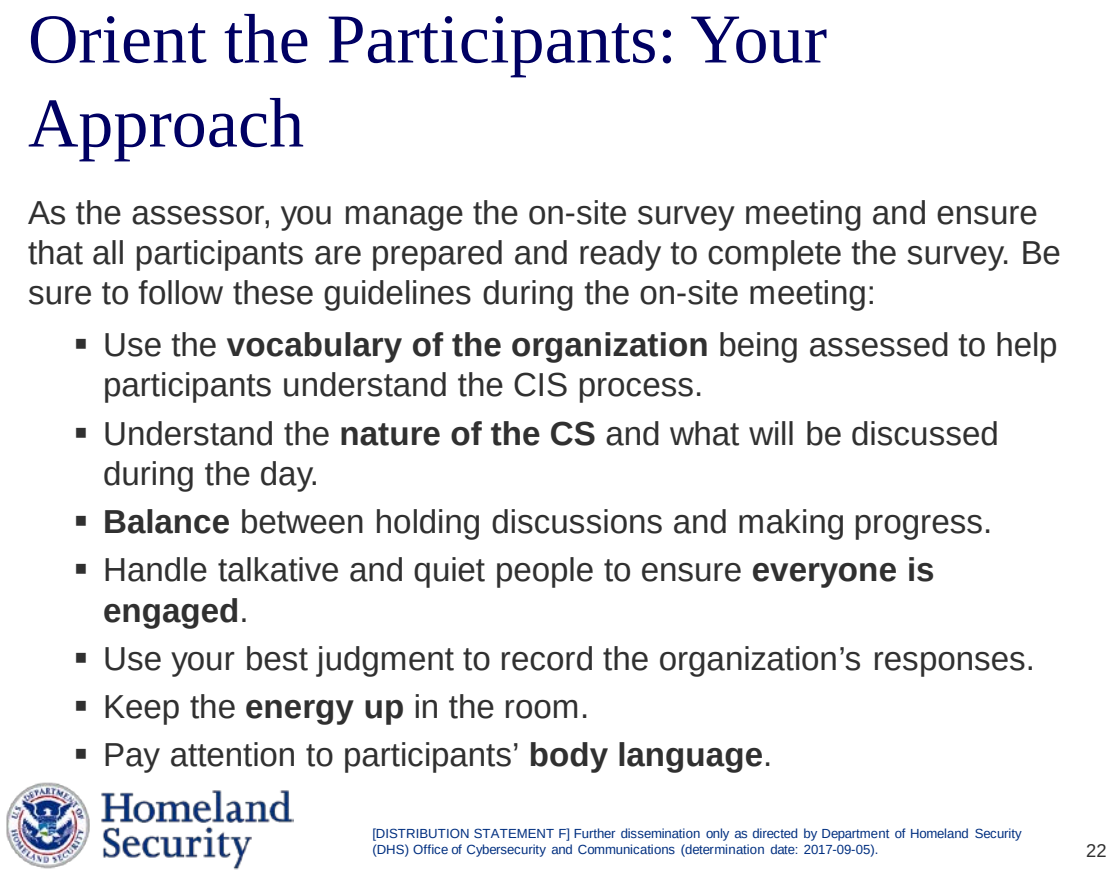
Before you get onsite, learn more about the organization and industry. Look at their website, see what you can gather. Do they have their mission, vision, values documented on their website? Industry, the sector-specific plans-- you can get a better idea of what that sector-- the main functions that sector is trying to achieve.

And then practice meeting management skills that help participants remain engaged and contribute to a successful event. Throughout here, you kind of have to gauge the audience and make sure you're not losing them, balance how much discussion versus too little or too much discussion.

So a tip here is bring a paper copy of the survey in case there's any technical issues that prevent you displaying concept or if the IP gateway is down. Bring a paper copy

so you can at least record the information and transpose that later on.

Orient the Participants: Your Approach



**022 So orient the participants, what your approach should be during the day. Use the vocabulary of the organization being assessed. As you guys are going to go out to more organizations, you're going to get more familiar with the lingo in the water industry and healthcare industry. Try and use their vocabulary to make it more real to them and provide the examples to them.

Understand the nature of the critical service and what will be discussed during that day. Kind of goes back to have them explain it one more time, make sure everyone in the assessment is operating from the same viewpoint.

Again, balance between holding discussions and making progress. In some of these assessments, you can go down rabbit holes. It's your job to kind of pull them back in, and whether you provide a briefing note or a comment saying, "Hey, I'll make a note of this, but I'm going to answer it this way. Let's move on."

Handle talkative and quiet people to ensure everyone is engaged. Sometimes if there's some people that are just in the room and they're not saying too much, I'll randomly ask them, "Do you agree with this? Is this how it's going?" Try and get other people engaged if they're willing to be engaged.

Use your best judgment to record the organization's response. Just because they're telling you something, you can say, "Hey, I'm making a comment. This is really what I'm hearing. I will note this as such."

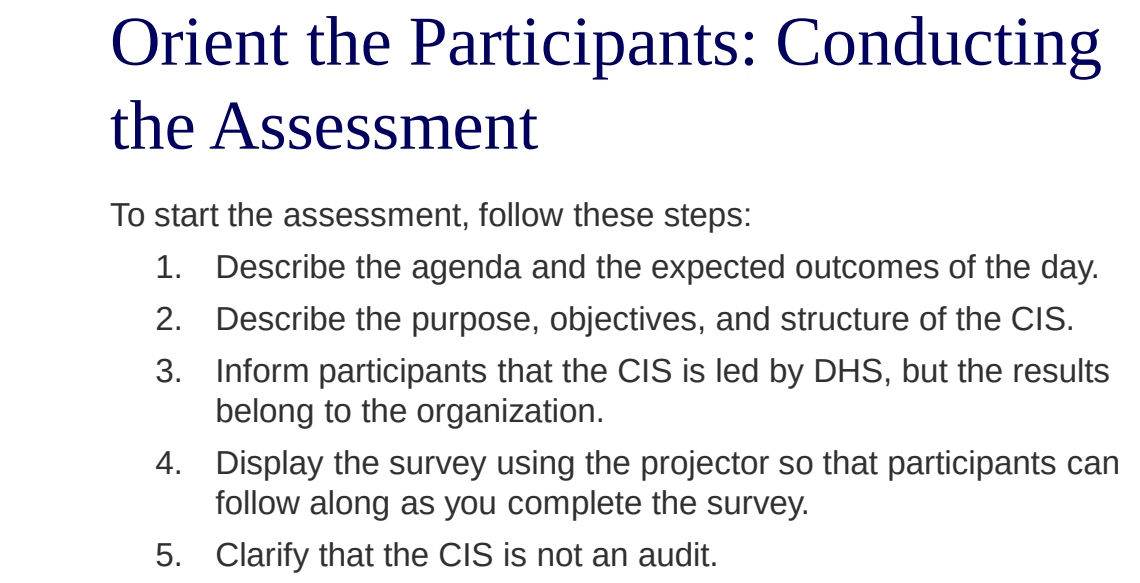
Keep up the energy in the room and pay attention to body language. So when you're losing anyone or taking too long, just kind of read the room.

Instructor: I would also go back and focus on understanding the nature of the critical service. It might be a few weeks since you've had

your last call. There might be additional people in the room. Maybe there's one or two more people in the room; they weren't part of that call. It's a very good practice to kind of review that again and make sure everyone's on the same page before you start the survey so that when you're telling them you need to be answering in relation to just the critical service as we described it, everyone's heard that description.

Instructor: Any other questions?

Orient the Participants: Conducting the Assessment



**023 So conducting the assessment. To start the

assessment, describe the agenda and expected outcomes of the day. Again, we've covered a lot of this. Describe the purpose, objectives and structure of the CIS. Inform them that this is led by DHS but the results belong to the organization. Display the survey using a projector so the participants can follow along as you're going through the survey. And then clarify that the CIS is not an audit. Based on some people's experiences, as you get in these organizations, and some people become defensive. If they're not doing a lot of these things, they become defensive. You just got to clarify, "Hey, we're here to help you. This isn't being used for regulatory. It's not an audit. It's truly for your benefit to kind of get better, to start doing the things you're not doing." So just clarify-- there's some times where you have to clarify it's not an audit and try and deal with defensive people in that way.

Orient the Participants: High-Level Review –1

Perform a high-level review of the survey contents, covering each section with the participants. Include the following with your review:

1. Review the CIS domains.
2. Remind participants that organizations that effectively manage cybersecurity risk may not need to perform all practices.
3. Review the survey-completion process.
4. Remind participants that they should answer questions based on the current state, not on past or future states. For example, answers should describe
   - controls that are implemented on the day of the evaluation and
   - practices being completed, not what can be done.

**024 Perform a high-level review. So again, review the domains. Remind participants that the organization, to effectively manage risk, you don't need to be doing all the practices. You have to take a look at your organization, what makes sense for them to be doing. Review the survey completion process. So we have checkbox-type questions. Some of the, "If yes..." we're going to drill into further detail. Let them know about the Comments section. Anything they want management to see, you can capture in the Comments section. So let them know how all the different

questions are going to be asked and answered.

And then this is important too: Remind participants that they should answer questions based on the current state-- not a past or future desired state but controls that are implemented on the day of the evaluation and practices that are being completed, not what can be done. Sometimes with logs or whatever they're saying, "Well, we could do this every day," but they're really not, so focus on what's currently being done and if you need to capture any type of comment, say, "This can be done." Maybe they need to establish it procedure-wise to do it, but focus on what's currently being done.

Instructor: Right. They may be building a capability that'll be available in 30 days. So it's a point-in-time assessment, so today the answer would still be no, but you can note in the comments that this capability is coming online on this date, right? So that work does get reflected in the results that they see.

Instructor: Any questions?

Orient the Participants: High-Level Review –2

5. Review the CS.
6. Review the assets listed that support the CS.
7. Explain how the CPRI is determined in the CIS dashboard.

**025 Again, review the critical service. Review the assets listed that support the critical service. And then also explain the CPRI and how it's determined in the final dashboard that you're going to be delivering them. But just kind of give a brief understanding so they understand as you're answering these questions the different controls are weighted, not everything is treated equally for some of these, but give a general description of that to the organization.

Orient the Participants: What to Expect

Explain to participants that, in the survey, they will see the following:

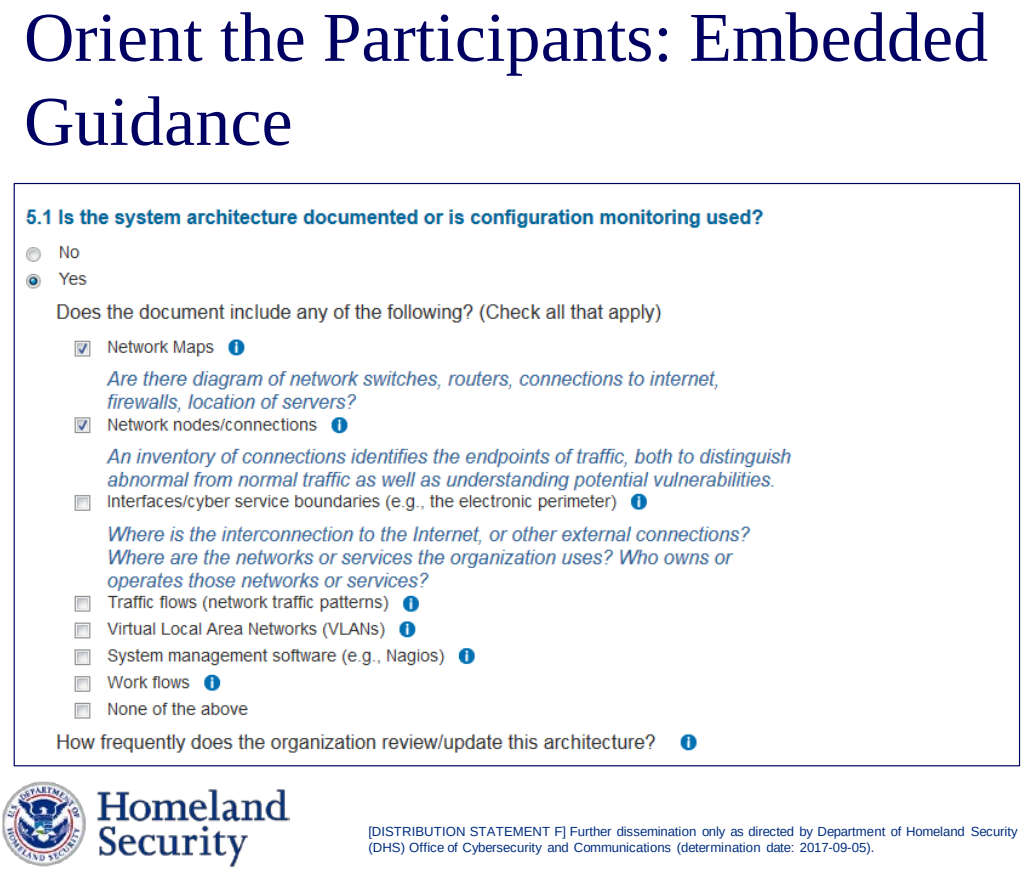
- Each domain is in its own section.
- Each question requires a response.
- Some questions have a parent and dependent-child relationship.
  - All parent questions must be answered.
  - All dependent questions must be answered when a parent question is answered.
- Each question has embedded guidance.

**026 So what to expect. Explain to the participants that each domain has its own section. Each question requires a response and also some questions have parent and dependent-child relationship. So all parent questions must be answered, and then all dependent questions must be answered when a parent question is answered. So if you select a Yes and multiple questions pop up underneath that, you need to answer all the questions underneath that-- for all those dependent questions.

Also, each question has embedded guidance for the assessor as well as

for the participants to follow along with.

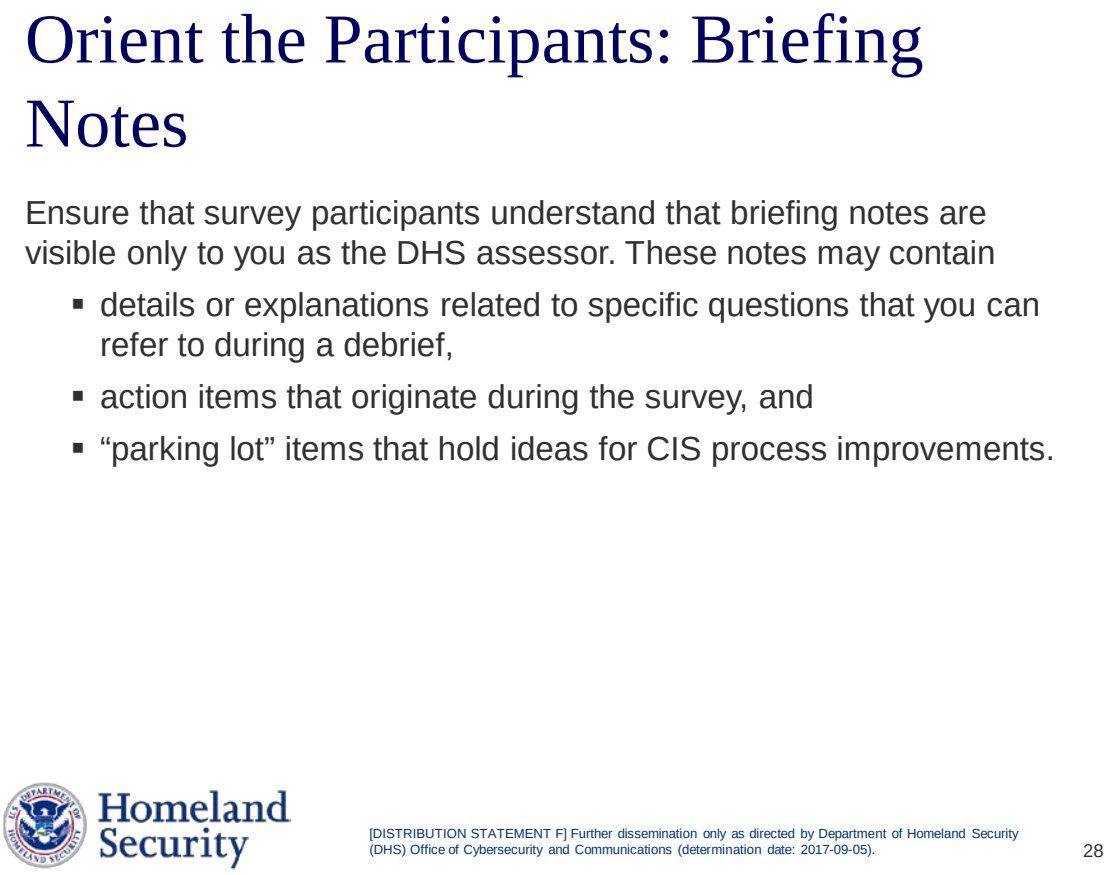
Orient the Participants: Embedded Guidance



**027 So that takes the form of what you see on the screen here. You can see that 5.1 has the actual question that you're asking. It also has the responses, but notice the blue highlighted circle with the "I" in it. If you click on those little dots, the selection expands and that blue text shows up. So it kind of can guide your information. If you're not as familiar with certain things, it can guide the information that you give to the organization, and pretty much everything has it. So these ones

down here we didn't expand, but you can see what type of guidance is given in those selections.

Orient the Participants: Briefing Notes

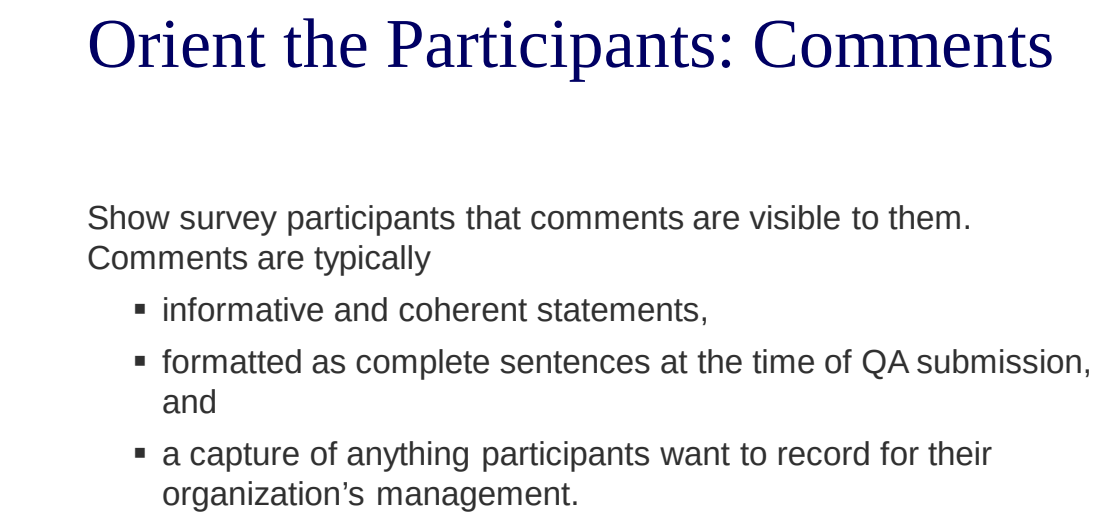


**028 So briefing notes. Ensure that survey participants understand briefing notes are visible only to you as the DHS assessor. So throughout the day you may be capturing some briefing notes. Things that you should be capturing here are details or explanations related to specific questions that you want to refer to during a debrief but don't necessarily want the organization to see all the detail you're putting. Any action items that originate during the

survey. If you're going along and you see a typo or any type of problem with a question, you probably want to put it in briefing notes to send back to whoever's handling QA aspects of the assessment.

Also parking lot items that-- well, that's basically what I just said-- CIS process improvement, parking lot items.

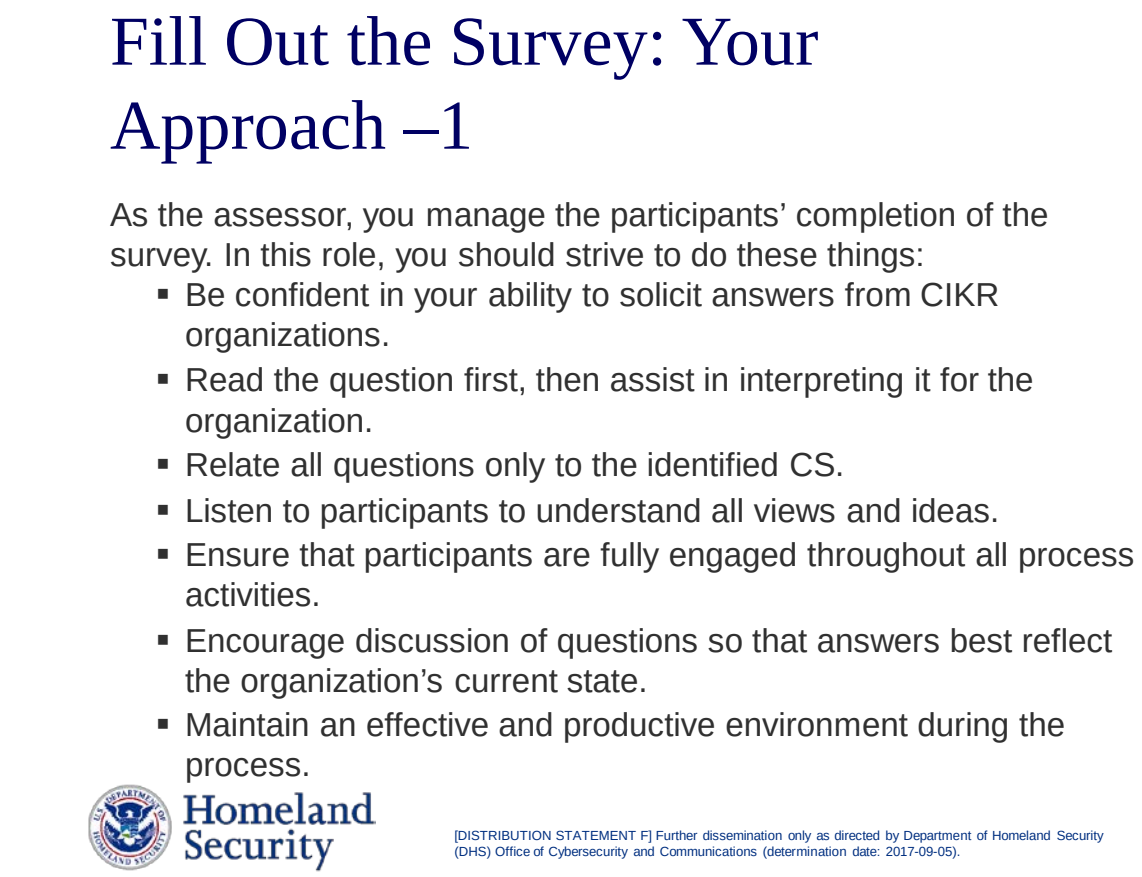
Orient the Participants: Comments



**029 So comments. As explained before, the comments are going to be visible to the organization after the dashboard is delivered. So make

sure that the statements you collect in there are informative and coherent statements. You don't want any shorthand or just little reminders that remind you of what you were talking about. Make sure they're informative and coherent, formatted as complete sentences at the time of QA submission. That's one of the things QA is going to be looking at, to see what's in the Comments section. And then capture anything a participant wants to record for their organization's management.

Fill Out the Survey: Your Approach –1



**030 Filling out the survey, your approach. So as the assessor, you

manage the participants' completion of the survey, so you should be doing the following things. So be confident in your ability to solicit answers from the organizations. Obviously this comes with practice, but be confident in asking the questions, explaining the different concepts. Read the question first. Read exactly what the question says and then assist in interpreting it for the organization. Try not to ad lib when you're asking the questions; read what's down there.

Relate all the questions only to the critical service. Again, as the day progresses, sometimes the conversation drifts. You want to make sure that everything is related back to that critical service.

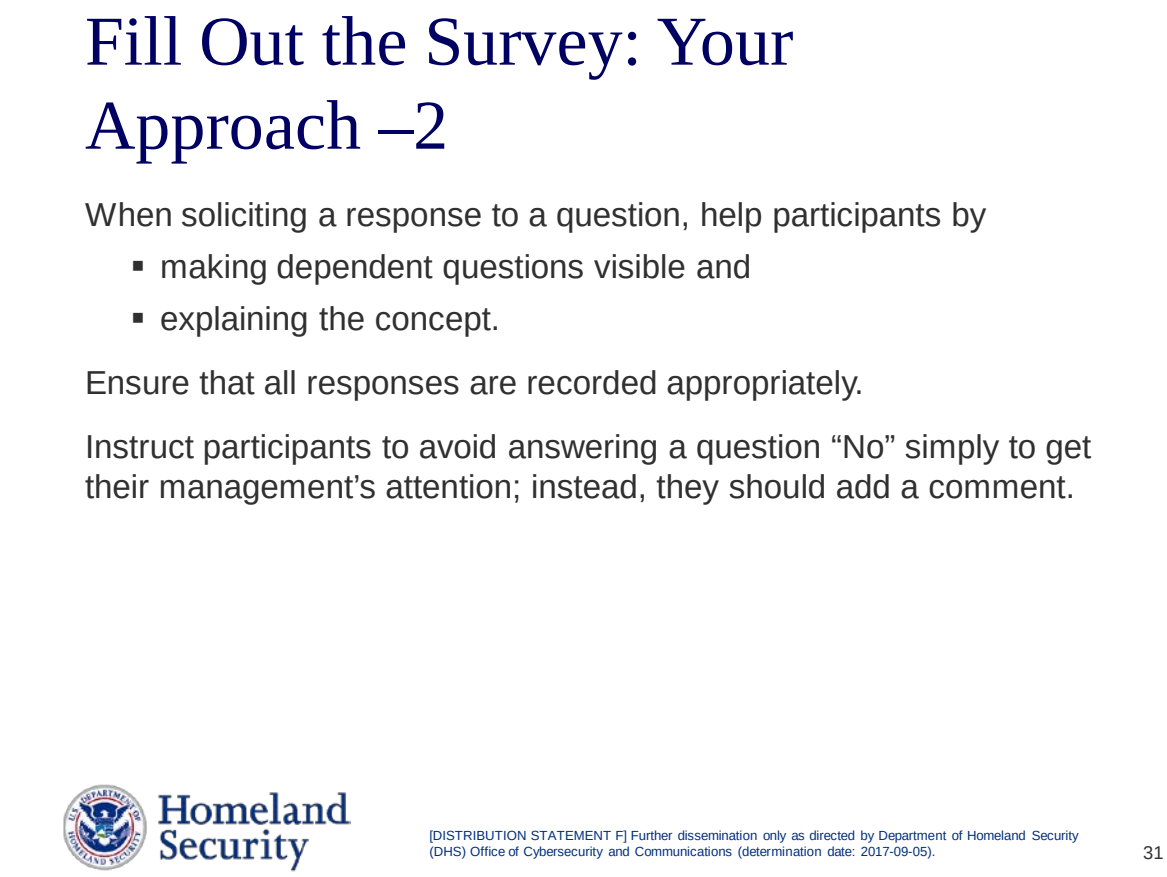
After you ask the question and kind of explain, you want to listen to all the participants and understand all views and ideas. As we talked about earlier, there's a tendency for the best practices to kind of bubble up right away, but listen to what the other people are saying. Sometimes managers are saying, "Hey, we should be doing it according to this," but then you have the day-to-day guys in the room and they're saying, "Well, it is supposed to be that way, but realistically we aren't doing this." So be sure you listen to everyone in the room.

Ensure that all the participants are fully engaged. Encourage discussion of questions so that answers best reflect the organization's current

state. So a lot of the times you'll provide your examples and you'll sit and listen. So encourage that discussion. Again, this isn't an audit. It's for their benefit. So sometimes having different people in the room, they talk-- they don't normally get a chance to get together and talk about these things, so encourage discussion.

And then maintain an effective and productive environment during the process.

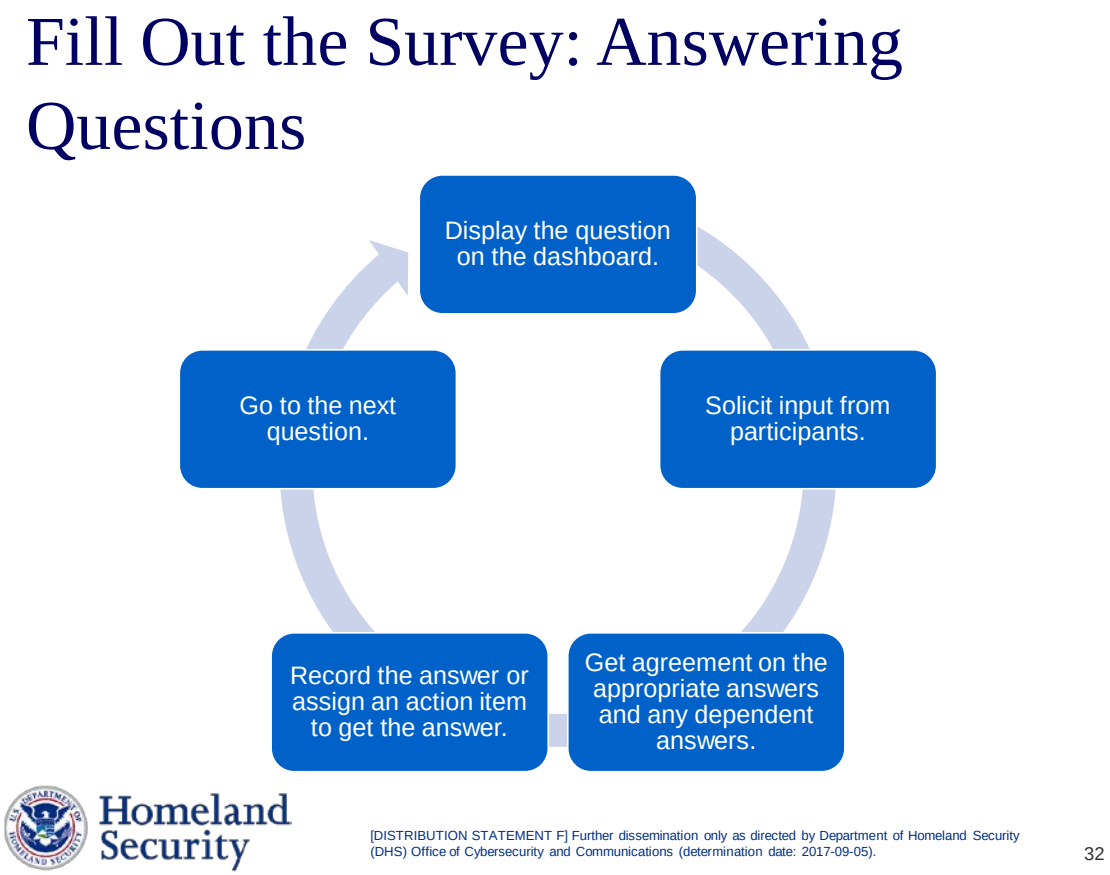
Fill Out the Survey: Your Approach –2



**031 When soliciting a response to a question, help participants by

making dependent questions visible and explaining the concept. So one of the techniques that's especially useful is, in the portal, when you're doing the survey, you'll see the high-level question, ask the question, and it'll either say Yes or No. As soon as you hit Yes, it's going to expand all the dependent questions. A good technique is to hit Yes right away and the organization can see the dependent questions. So they may not know what you're talking about with the base practice question, but if you expand everything, it helps them follow along, and if it's truly a no, then it's a no, but they can see all the other build-ons. So it might clue them in to more of what you're asking.

So instruct participants to avoid answering a no simply to get their management's attention. So if they're saying-- if they're doing something maybe ad hoc, you want to give them credit for the ad hoc-- you don't want to say, "No, they're not doing that." If they say, "Hey, let's just put a no here, we're not doing that," it might be more appropriate to say, "Well, this is currently what's in place. We answered it this way." So a better practice would be creating a comment that you can present to the organization in the Comments section.



**032 So again, kind of flowchart for answering questions and asking the questions. Display the question on the dashboard. You want to solicit the input from the participants, get agreement on the appropriate answers and any dependent answers. So particularly for this assessment, a lot of the times you're displaying it up on a screen. So either explain why you're answering something a certain way or get agreement from everyone on how you're going to answer this. Record the answer and assign any action to get the answer, whether you use briefing notes or comments for that. Go to the next question.

Fill Out the Survey: CPRI

As participants answer the survey questions, the CPRI dynamically adjusts so that all participants can see how their answers affect it.

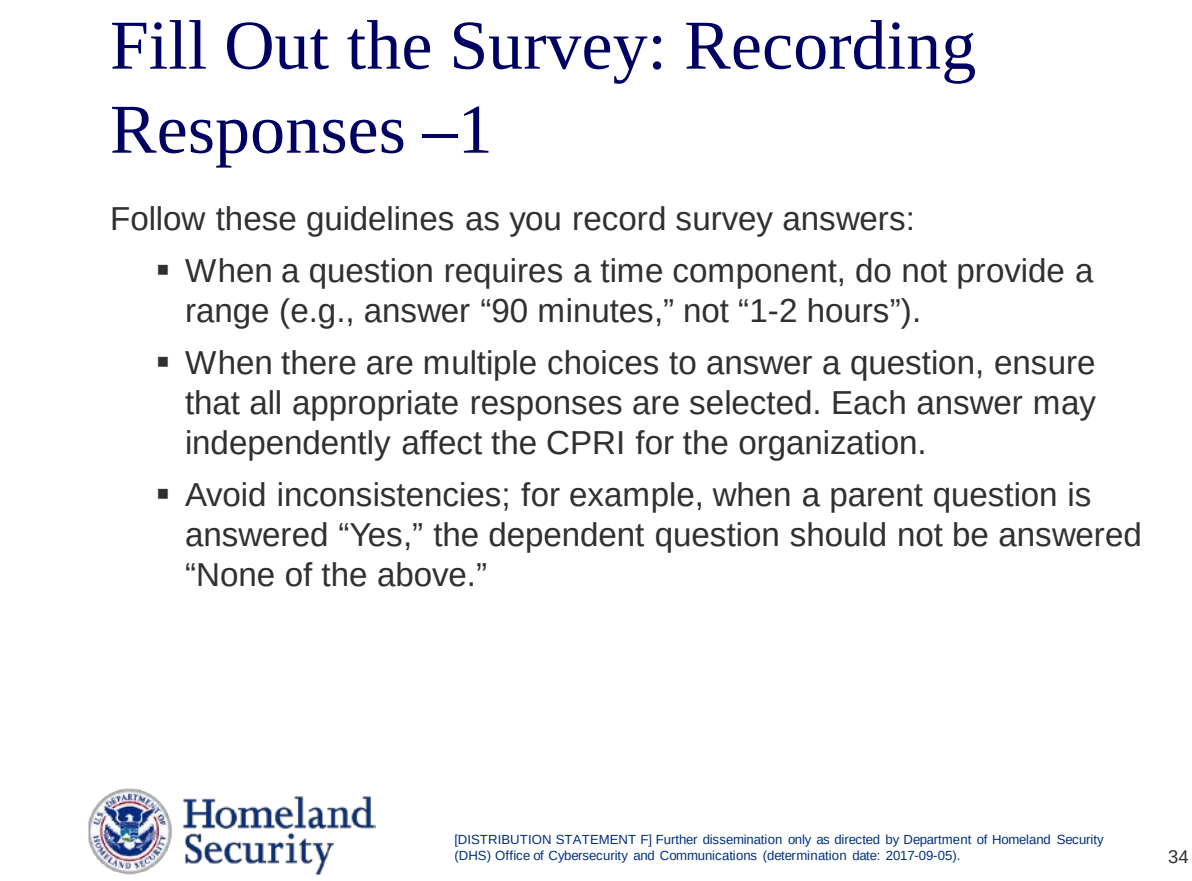
**033 So as participants answer the survey questions, you can see the CPRI dynamically adjust, so you can see how the different practices affect it. Basically when you're asking these questions, there's going to be a bar above each question that gives the CPRI-- it's not the dashboard but it kind of shows you if you answer this best practice, the weighted values almost. You can't really see what's underlying there, but you can see that maybe having a documented process, you're going to jump to 20 percent, whereas if you're only doing something ad hoc, it might only add 5 points to the CPRI score.

Student: It gives you a quick indication? Like a real-time indication of where you are.

Instructor: Right, and you can use that as teaching tools to the organization then and say, "Okay, well based on this methodology, what you're doing is really only this effective in some ways. If you just spend a little more resources here, based on this methodology, this is giving you a lot more bang for your buck."

Any questions on CPRI?

Fill Out the Survey: Recording Responses –1



**034 Recording responses. So some guidelines to keep in mind when you're recording answers.

When a question requires a time component, do not provide a range. Provide a whole number. So answer 90 minutes, not one to two hours or one and a half hours.

When there are multiple choices to answer a question, ensure that all the appropriate responses are selected. So whenever it says "Select all that apply" or, even in some cases where it doesn't, be sure to solicit all accurate answers because each section affects the CPRI score, either positively or negatively, but you want to give them an accurate portrayal of what they're doing.

So avoid inconsistencies. For example, when a parent question is answered Yes, the dependent question should not be answered with something like "None of the above."

Student: Would "None of the above" even be a dependent question?

Student: Well, I could see that. I mean, if it doesn't have an Other-- you could have a bunch of conditions. You ask a question and they say, "Yes, but we don't do any of that."

Student: It should be Other, not None of the Above.

Student: There should be an Other where you can fill it in.

Instructor: Yeah, so--

Student: Conceivably-- but I can see the circumstance.

Instructor: Yes. This is why what we saw happening and we have in here is displaying that Yes-- selecting it even though they haven't answered yet so they can see the range of possibilities, helps them understand the question as well, and they get to see some of that, and they may say, "You know what? We do do this. I'm going to answer yes here." But just be cognizant that in most cases-- there are some cases where "None of the above" is appropriate, and we kind of point that out, but in most cases it would not be, and it just causes kind of a QA issue.

Instructor: And we have some more of those listed in the next section under Question Intent. Klint?

Student: So on the questions that require a time component, how much is the overall score changed-- I mean, how does it-- and this might not be a question that you can answer-- but if you put down that the system has a mean time to restore of 90 minutes versus 7 hours, is it actually looking at whatever you type in there and using that as a scoring mechanism, or is it just looking that you typed something in, and that's more for our benefit in a data point for us later on?

Instructor: Yeah, we really don't have a view of what those weights are and to know, to your point, is it-- if I select that I'm doing something

more often, is the weight heavier than if I say I'm doing it monthly, versus I'm doing it daily, right?

Student: I'm thinking about the places where we're actually typing in the time.

Instructor: Yes. So you're typing in 90 minutes versus 1 day. Right? So we don't have a real view to know if those are weighted differently. So unfortunately we-- that was one of the things that we talked about trying to get, but we don't have that, to be able to answer that yet.

Instructor: You could do it. After you generate it, just for the heck of it, you could just change the answer.

Instructor: Yeah, and you can see the effect.

Instructor: Any other questions on recording responses?

Fill Out the Survey: Recording Responses –2

- When a question is answered “Other,” add clarifying text as requested.
- In the Frequency Information field, “Continuously” means that it is done in an automated fashion.

Caution

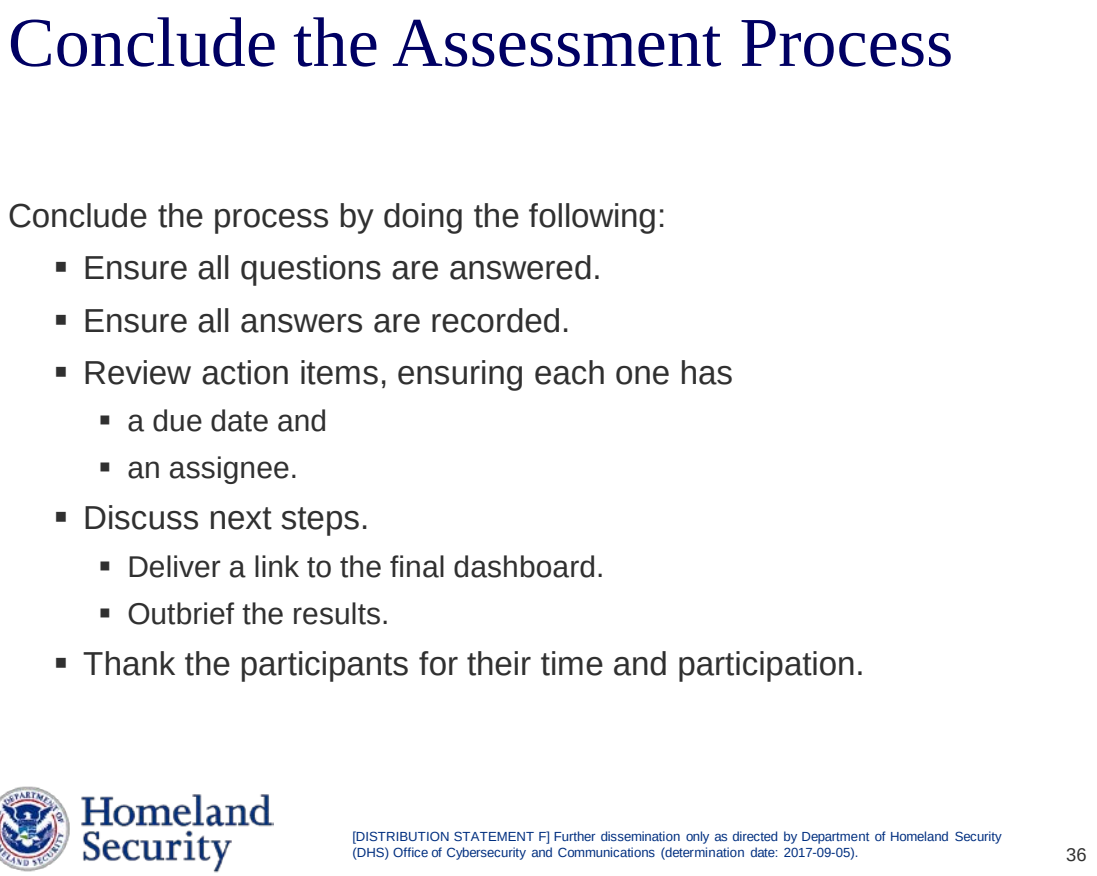
The CIS allows for inconsistencies. As the CIS assessor, you should be prepared to reverse a previous answer to ensure answers are correct and consistent.

**035 So another thing to keep in mind, when you answer a question as Other, be sure to add clarifying text to add more detail to that Other selection. In the Frequency Information field, "continuously" means that it is done in an automated fashion. We kind of hit on that earlier, but "continuously" is really looking at something that's automated in a continuous fashion.

So be aware the CIS allows for inconsistencies. So as the assessor, you should be prepared to reverse a previous answer to ensure answers are correct and consistent. We'll get into some of these inconsistencies in

the next section, but just be aware that you have to manually go in and change the answers based on maybe new information as you're going along in the assessment. You have to change those answers.

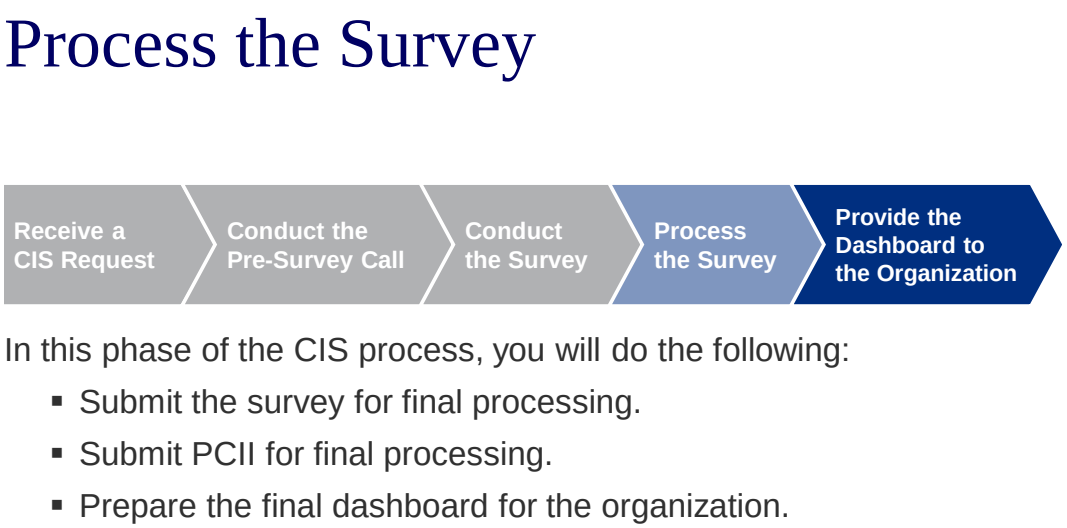
Conclude the Assessment Process



**036 So at the end of the day, you're going to want to ensure that all questions are answered. You're going to want to ensure that all answered are recorded. Review any action items, ensuring each one has a due date and an assignee. You then want to discuss the next steps-- so when you're going to deliver the link to the dashboard-- offer to

outbrief the results, and then, again, thank the participants for their time and participation.

Process the Survey



**037 Instructor: The next section is to process the survey. So in this phase, you will do the following: submit the survey for final processing, submit PCII for final processing, prepare the final dashboard for the organization. So this lines up with Phase C in the workflow of the IP Gateway portal.

Provide the Dashboard to the Organization

When you provide the dashboard to the organization, you do the following:

- Review the draft dashboard for accuracy.
- Finalize the dashboard.
- Initiate dashboard delivery.
- Conduct a debrief call.
- Review additional DHS capabilities that are available to the organization.

Homeland Security

**038 And then the last section is provide the dashboard to the organization. Before you send the link, review the dashboard for accuracy. Finalize the dashboard. Initiate dashboard delivery. Conduct the debrief call, and review additional DHS capabilities that are available to the organization at this point. So whether this is the first engagement with the organization or not, offer the different assessments, the different information-sharing you guys may be able to provide them to further assist them.

Student: Do we provide the dashboard at a later time, or is it directly after the--

Student: It's part of the flow. As you're going through IP Gateway, it'll have-- you'll see as it goes through, and one of the things you'll click on is essentially giving them the...

Student: If you're offline, do you sent it at a later time? If you're offline during the--

Student: Yeah, you would have to.

Instructor: This would take place not the day of.

Student: Yeah, because it's going to have to go through quality assurance check too. So once you finish the dashboard, you submit for QA. QA takes a day, two days, three days, depending on the backlog.

Student: A week or two.

Student: Yeah, a week, right?

Instructor: Depending on the backlog it can take some time, and then you'll get a notification that you've passed QA, and then you also have to wait for your PCII to be set up.

Instructor: Yeah, you may indicate that within 30 days or three weeks. I mean, what do you guys typically indicate?

Student: I tell them our own guidelines are no greater than 30 days and they should have it, and in most cases I've been able to get it to

them no later than-- three weeks one time, but that was because...

Student: But you can also ping ops and say, "Hey, I got"-- because I got five sitting in QA because they're all here. And so you can ping ops and everything and get a response. But back to your point on conducting the survey was offline capability. That's an issue where there's not a-- you got to be hooked into the mothership in order to conduct the survey, and so that-- there's not a real good methodology for an offline capability as of yet.

Student: Well, I would say there is the PDF. I mean, it's not the best.

Student: But you got to transcribe.

Student: That's essentially paper. You're doing it by paper at that point.

Student: Yeah, because you might be somewhere in North Dakota. Just there's no internet.

Instructor: Right. So there is a difference in some of the other assessments. There is an offline capability, right? But not here. To Tony's point, there is a PDF form that will capture the data for you, but there's no export capability or import capability into the portal.

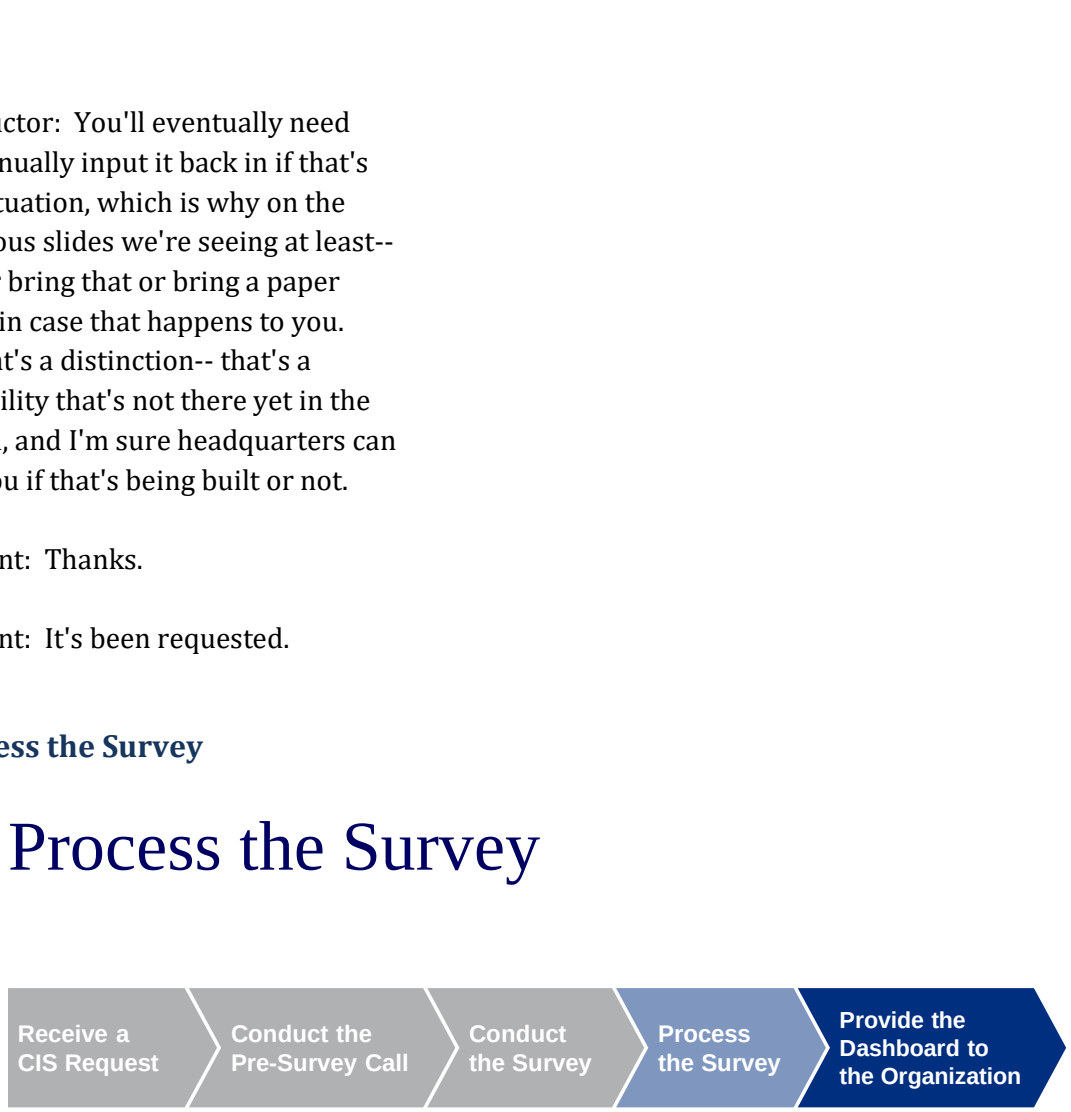
Student: So we can do it in writing but we have to manually input it eventually.

Instructor: You'll eventually need to manually input it back in if that's the situation, which is why on the previous slides we're seeing at least-- either bring that or bring a paper copy, in case that happens to you. So that's a distinction-- that's a capability that's not there yet in the portal, and I'm sure headquarters can tell you if that's being built or not.

Student: Thanks.

Student: It's been requested.

Process the Survey



**037 Instructor: So one thing I did want to hit upon in the Process

the Survey, at this point you're going to be-- this is where you attach the PCII Express and Certification statement. So whatever is on that signed form, make sure that the name and contact information is the same as the paper copy as what's in the section of the portal as well.

Instructor: Right. So realize that some of that gets prepopulated, I believe, depending on what you put in early phases, for like contact information and so forth. But the people signing it in the organization may end up being different. So this is one point that becomes a QA aspect, right? It needs to be the same. So it's something you should go back and check, to Gavin's point, to make sure that happens.

The CIS Engagement Summary

As you manage the CIS engagement, you should accomplish the following:

- ✓Form a relationship with the organization.
- ✓Identify and discuss the organization's CS.
- ✓Gain insight into the organization's cybersecurity concerns and the scope of the CIS process.
- ✓Collect demographic information.
- ✓Manage completion of the survey.
- ✓Confirm that the survey and answers are complete.
- ✓Complete the QA and PCII processes.
- ✓Provide the organization with a link to their dashboard.
- ✓Debrief the organization.

Homeland Security

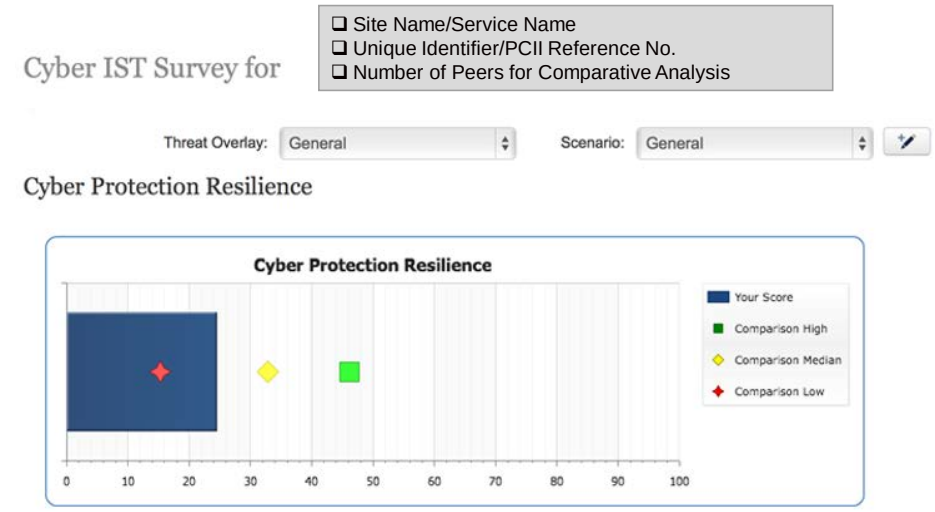
**039 Instructor: Okay, in summary for the CIS engagement, really you're forming a relationship with the organization. You will have discussed and identified the critical service, collect the demographic information for the organization, manage the completion of the survey, and at the end provide the organization with a link to their dashboard and debrief the organization on the results, offer any further assistance you may be able to offer.

CIS Dashboard

Table of Contents

**040 The CIS dashboard.

The CIS Dashboard: Layout –1

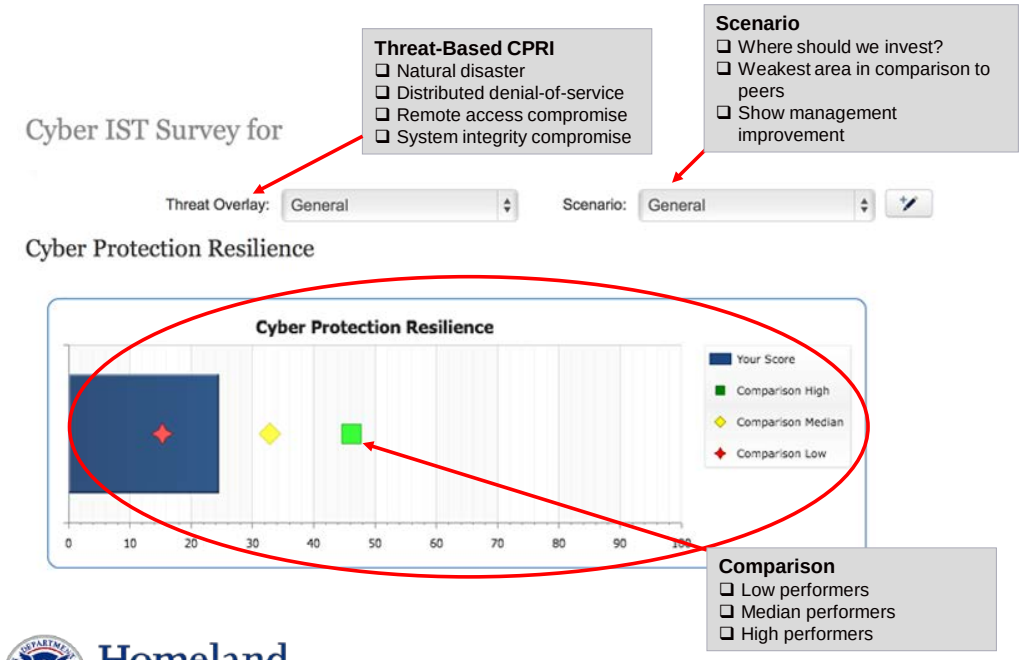


Homeland Security

**041 So here's a high-level overview of the layout of the dashboard. You can see that it says "Cyber IST Survey for". This is still what's in the portal as of today. So it'll give the site name or the service name. It provides the unique identifier, PCII reference number for that assessment, and number of peers used for the comparative analysis.

Different layout sections. Here's the threat overlay, scenario overlay. Here's the CPRI score along with the different comparative analysis with low, medium and high performers.

The CIS Dashboard: Layout –2



Homeland Security

[DISTRIBUTION STATEMENT F] Further dissemination only as directed by Department of Homeland Security (DHS) Office of Cybersecurity and Communications (determination date: 2017-09-05).

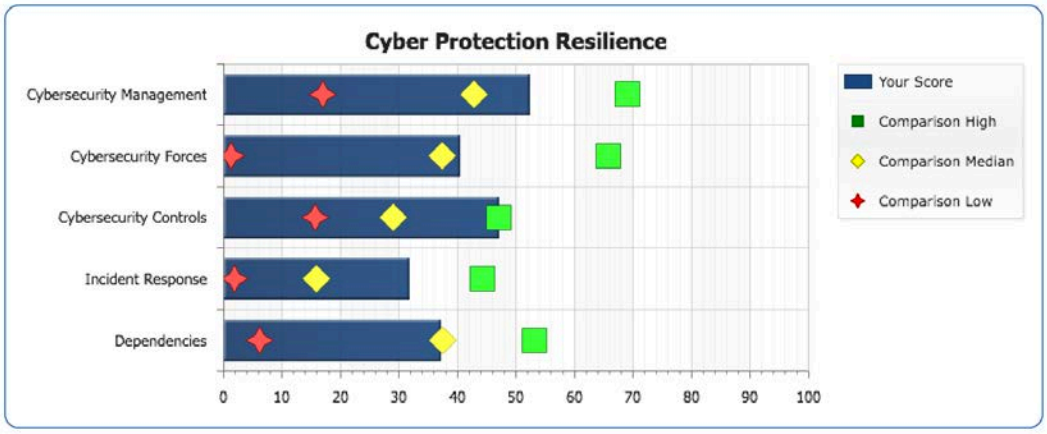
42

**042 Kind of hit upon all those already.

The CIS Dashboard: Peer Comparison

The CIS dashboard

- shows the low, median, and high performers and
- compares your organization to like organizations.



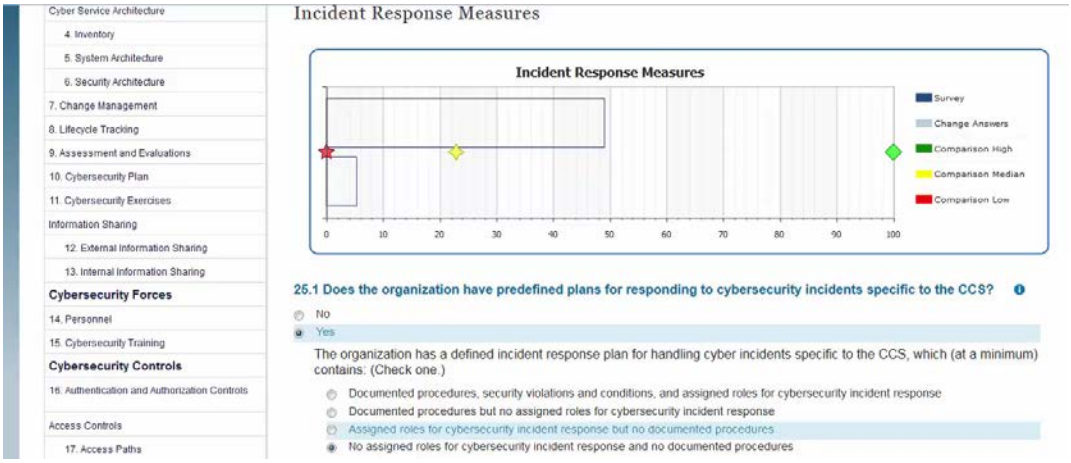
Homeland Security

43

**043 Again, here's the dashboard at the domain level. So again, it shows the low, medium, and high performers, and it compares your organization's with like organizations.

The CIS Dashboard: Scenario Planning

The CSA can dynamically display CPRI values and how different practices can affect them.



Homeland Security

**044 So one of the things previously I mentioned is you as the assessor can show dynamically how different practices affect the CPRI values. So here's an example of somebody going through the assessment and as they change the answers, you can see how the CPRI on the bottom is changing states. So in this case, as you're moving up, the more weighted practices are-- and this is true for most of the assessment-- the higher-weighted practices normally show up first.

The CIS Dashboard: Threat Overlays –1

The dashboard considers all cyber hazards and threats equally when a threat overlay is not selected.

You can extend CPRI information through threat ‘overlays’.

- Overlays relate a limited number of cyber threat types to the CPRI.
- For example, how does the effectiveness of practices change when dealing with a DDOS attack?

Homeland Security

**045 So you can also extend CPRI information through threat overlays. So by choosing these overlays, you can see how effective certain practices are or are not against certain threats. An important thing to consider is the dashboard considers all cyber hazards and threats equally when a threat is not selected. So there's no weighting on any type of threat scenario whenever you're not using one of the four threat scenarios built into the dashboard.

So you can use this: "How does the effectiveness of your practices in place change when you're dealing with denial-of-service attack?"

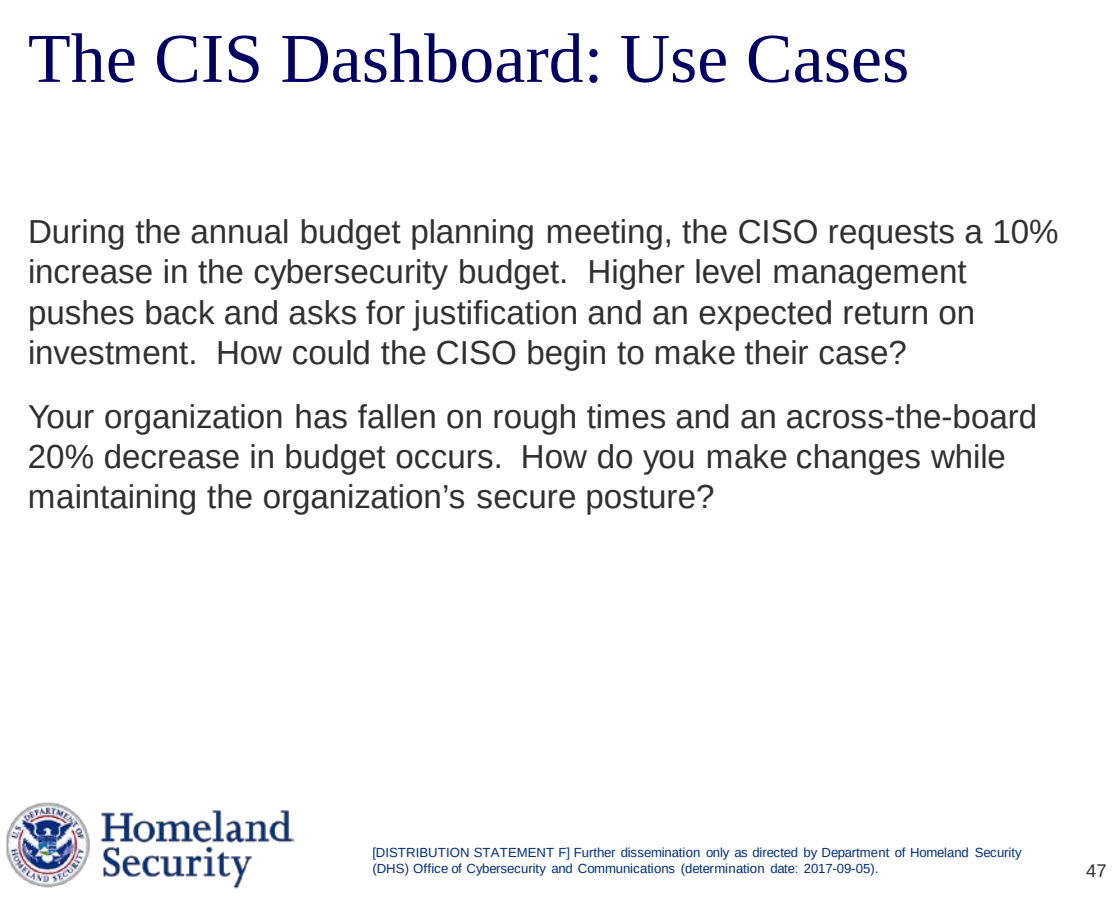
The CIS Dashboard: Threat Overlays –2

Examples of threat selections are

- malware that compromises applications that directly support the CS by allowing unauthorized remote access,
- DDOS directed using a botnet from a foreign ISP,
- destructive malware that enables the destruction of data, and
- a natural disaster that affects all physical assets related to the delivery of the primary CS.

Homeland Security

**046 The threat scenarios that are built into the dashboard are malware that compromises applications, that directly support the critical service; a denial-of-service attack; destructive malware that enables the destruction of data; and then also a threat for a natural disaster that affects all physical assets related to the delivery of the critical service.



**047 Also you can have use cases that you can present to the organization to help them use the dashboard to their benefit. So here are examples of two use cases. So, during the annual budget planning meeting, the CISO requests a 10 percent increase in the cybersecurity budget. Higher level management pushes back and asks for justification and an expected return on investment. How could the CISO begin to make their case?

They can start making scenarios within the dashboard to say, "By doing this, we're getting more bang for our buck, because this practice or

this tool may provide more protections than what we're currently doing."

Alternatively, you can use it when your organization has fallen on rough times and an across-the-board 20 percent decrease of budget occurs. How do you go about making changes while maintaining an organization's secure posture? So if you have to cut things, you can kind of use it as a decision support tool to say, "Should we be cutting this or not?"

The CIS Dashboard: Scenarios

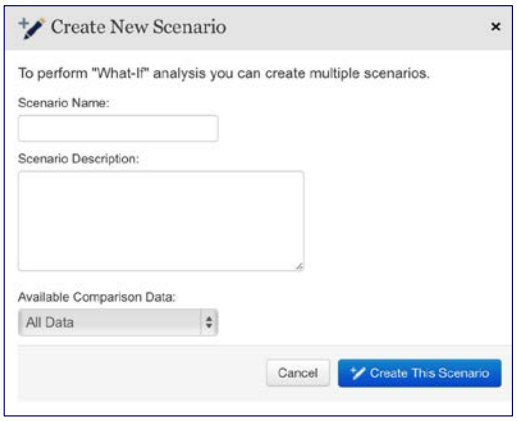
The CIS Dashboard: Scenarios

A feature of the CIS is the ability to create scenarios.

- Creating scenarios based on use cases allows an organization to examine the impact of changes.

Scenarios can help the organization determine

- where to invest to buy down risk,
- where the weakest area is in comparison to its peers, and
- how to show management the gains or losses by doing x or y.



Homeland Security

48

**048 Again, you can create these scenarios. If you hit the Scenario

button, you can name the scenario, provide a description, select which available comparison data is in there. So scenarios are really aiming to help an organization decide where to invest to buy down risk, where the weakest areas-- where they are weakest in comparison to their peers, and to show management the gains or losses by doing X or Y.

Student: Have you all-- and these are to my colleagues-- have you all found this useful?

Student: I haven't even used it yet.

Instructor: It depends. If you go to a domain where they answered No or Yes and you change the answer there, you'll see a huge change in the bar graph. If you're just changing one or two, at least in my situation, that's where I got the call coming back, "Hey Tony, the dashboard's not working." So it just really depends. But until we flush all that stuff out, they might have a specific reason to use that scenario and then go in and find out that those particular things that they're changing don't have enough weight to make a significant difference, and that's what I was trying to get to yesterday.

Student: Got it.

Student: So where people can use it, if they have multiple agencies and they want to assess-- do self-assessment, they can create a scenario and then rescore themselves based on-- right now it's the only way

we have to do it, if they want to do self-assessments with themselves, is to build a scenario inside the current assessment, or dashboard.

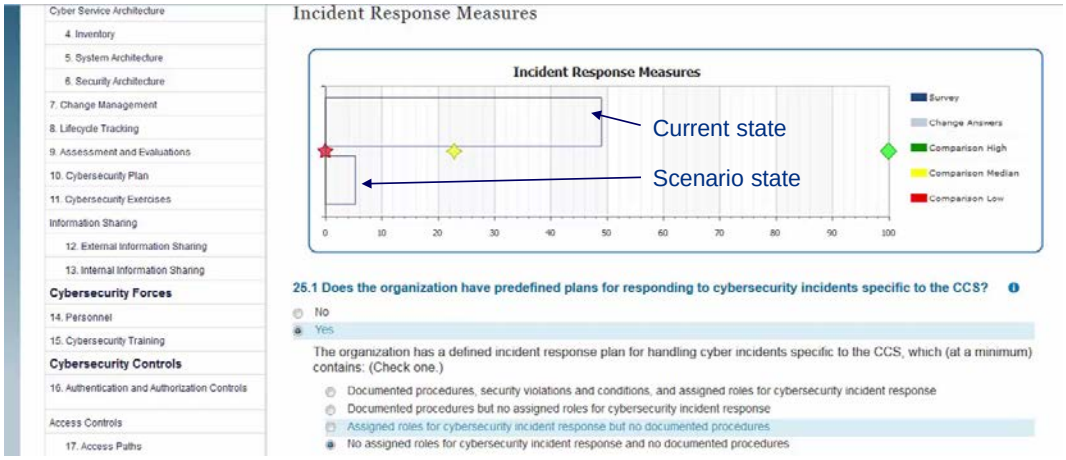
Instructor: Right. So realize what was said before-- what you're hearing them describe is that not all weights are equal, and if you recall the discussion on the dashboard and having those expert groups, how they viewed those practices against DDOS or an all-out event affects those weights differently, adjusts those weights differently. So to Tony's point, you may see very little change in some instances and then bigger in others depending on what the starting point was, and some of it could be so minor that it may not be noticed. Right?

Student: Right. Okay.

Use of Scenarios

The top bar represents the organization's current state.

The bottom bar represents the organization's scenario state.



Homeland Security

**049 Instructor: So again, here's a depiction of how the scenario and current states are represented. So on the dashboard when you enter the scenarios, you can do-- the current state is on the top and then the scenario state will change as you go through and select different answers.

Managing the Engagement: Objectives Summary

In this section, you learned

- the phases of the CIS engagement and management process,
- how to apply best practices and tips to manage the engagement, and
- how to use the dashboard to benefit the organization.

50

**050 So in summary for this section, we identified the phases of the CIS engagement and the management processes, how to apply best practices and tips when you're managing the engagement, and then how to use the dashboard to benefit the organization. That concludes this section.

Instructor: Any other questions based on what you saw this morning? So that scenario builder is one of the main benefits of the CIS.

Introduction

Table of Contents

Question Intent

September 2017

Homeland Security

**001 Instructor: Okay everyone, we're going to move into the last section of the training. It is also the longest. It's titled "Question Intent".

**002 [Notice]

Question Intent: Objectives

After completing this section, for each domain, you will understand

- concepts and terminology,
- training tips,
- QA aspects (e.g., know to watch for inconsistent responses),
- best practices, and
- how different areas of the survey support each other.

**004 So some of the objectives: To understand concepts and terminology for each of the domains. We'll be presenting some additional terminology here. Pass on some training tips. We're going to be looking at some of the QA aspects that are currently seen, and also present some of the best practices from an organizational point of view that you could pass on to people that you're doing this with. It's really kind of what the CIS is getting at when you look at the questions. And then also how different areas of the survey actually support each other or intertwine with each other.

Question Intent: Topics

Background

Cybersecurity Management

Cybersecurity Forces

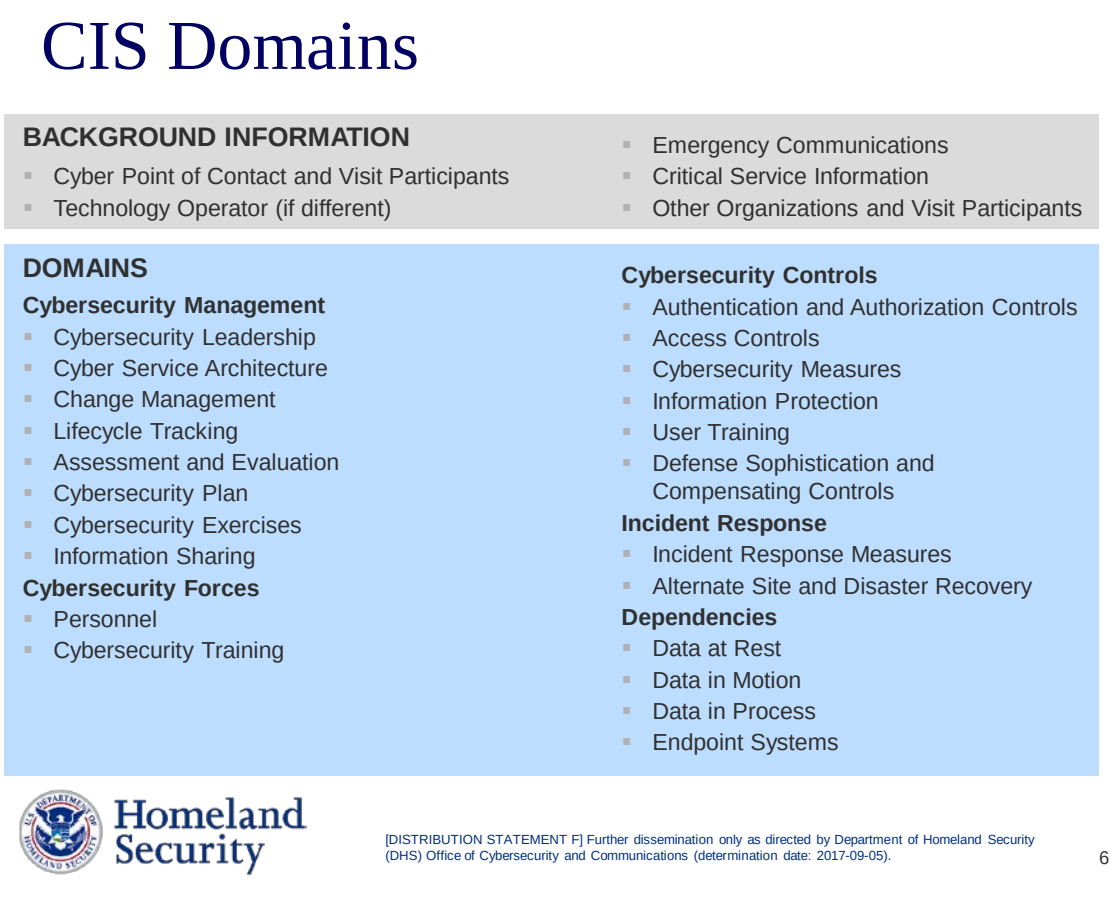
Cybersecurity Controls

Incident Response

Cyber Dependencies

**005 So we're going to do this for each one of the domains. We're going to walk through all six.

CIS Domains



**006 Again, just a reminder of what all the domains are and how they're structured.

CIS Domains by the Numbers

CIS Domain	Checkbox	If Yes	Text Input	Notes	Total
Background Information	27		35		**62**
Cybersecurity Management	28	47		22	**97**
Cybersecurity Forces	8	11		4	**23**
Cybersecurity Controls	24	55		16	**95**
Incident Response	9	7	1	4	**21**
Dependencies	5	36		8	**49**
Total	**101**	**156**	**36**	**54**	**347**

**007 Again, looking at the domains by the numbers, which ones are larger, relative size. It could help you when you're trying to plan out your day.

Background

Table of Contents

Background

Cyber Infrastructure Survey (CIS) Training Course

Homeland Security

**008 So let's start with the background domain.

Background Information Domain –1

This CIS domain is used to document information about survey participants, including their roles and contact information. It also describes the critical service (CS) that the survey will focus on.

**009 So the domain is used to document information about the survey participants as well as to establish what the critical service is. That's the intent of the domain, as we've kind of spoken to before.

Background Information Domain –2

Background Information Domain	Checkbox	If Yes	Text Input	Notes	Total
Cyber Point of Contact (POC) and Visit Participants	6		22		**28**
Critical Service Information	21		13		**34**
Total	**27**		**35**		**62**

This domain contains a total of **62** questions.

- There are 27 simple checkbox responses.
- There are 35 questions that require free text to be input.

**010 So this background domain is actually 62 questions long.

Cyber Point of Contact: Overview

Background Information Domain	Checkbox	If Yes	Text Input	Notes	Total
Cyber POC and Visit Participants	6		22		**28**

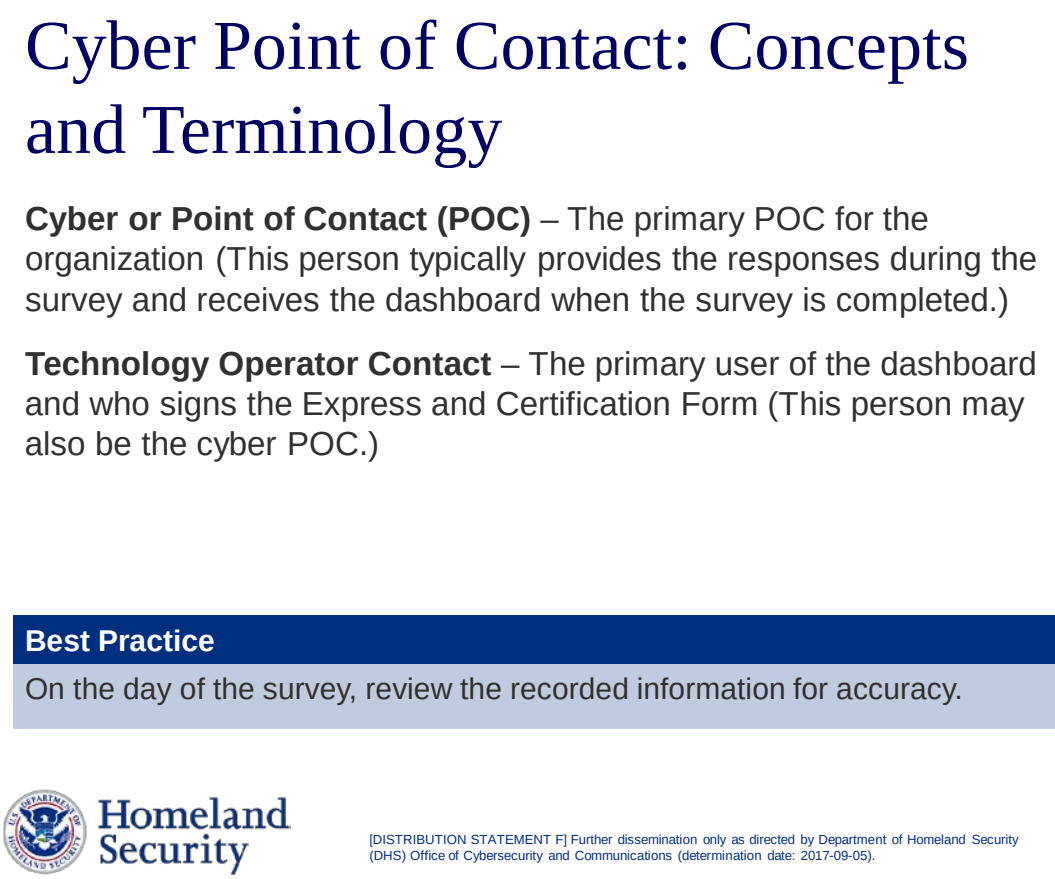
Most entries in this domain are demographic in nature and are completed during pre-survey calls and scoping activities.

Information collected includes

- contact information,
- location information, and
- names of additional participants.

Homeland Security

**011 Cyber Point of Contact: Overview. So most entries in the domain are demographic in nature and are, again, completed during the pre-survey call and scoping activities. Types of information collected is contact information, location, names of additional participants.



**012 Some terminology. There's a Cyber Point of Contact, which I believe is understood by everybody. However, there's a terminology in the CIS called Technology Operator Contact, and the primary user of the dashboard and who signs the express statement. That's how the CIS defines it. Often they could be the same person, but there is an additional role there that we thought would be good to bring out.

Again, the best practice, on the day of the survey, again, review the recorded information for accuracy. Make sure that that is still valid, especially the critical service. You

want to review that with the participants as well.

Student: So both the Cyber POC and the TOC will have access to the dashboard, if they're not the same person.

Instructor: So the dashboard is typically given to that main contact. So it would normally go to this Technology Operator Contact, and they have the ability to assign additional people that would have access to it.

Critical Service Information: Overview

Critical Service Information: Overview

Background Information Domain	Checkbox	If Yes	Text Input	Notes	Total
Critical Service Information	21		13		**34**

The CS provides the context for the CIS, so CIS questions should be answered as they relate to the CS.

Responses include

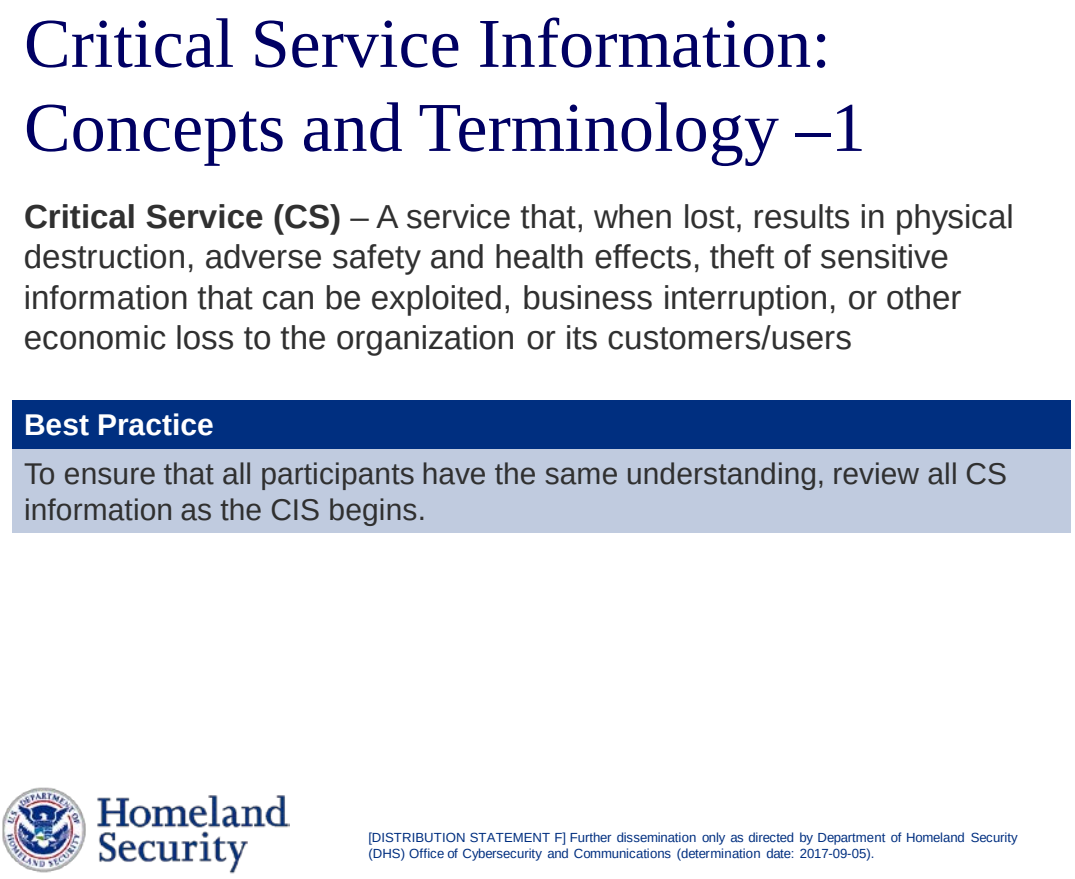
- description of the CS,
- number of the supporting staff, and
- descriptions of the network and its supporting applications.

Homeland Security

**013 Critical service information overview. It provides context.

You're basically providing the context for the CIS itself. The CIS is going to be asking questions relative to the critical service. So you're going to be, in this section, providing a description, things like the number of staff supporting the service, descriptions of network and other applications or technology.

Critical Service Information: Concepts and Terminology –1

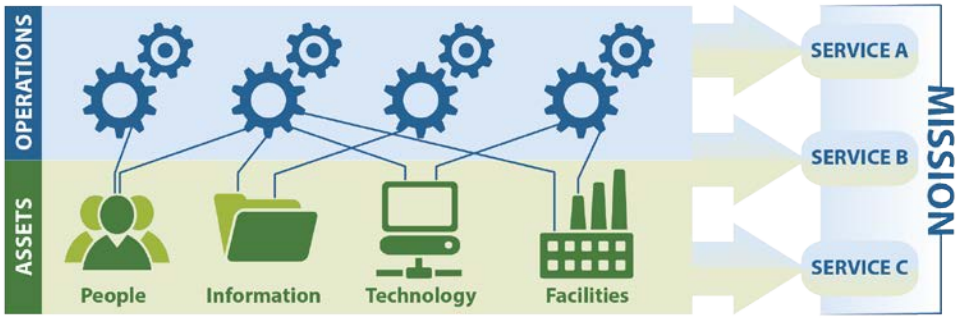


**014 Critical service information: Concepts and terminology. We've kind of reviewed this already. This is how the CIS is defining it, a service that when lost results in a physical destruction, adverse safety or health effects, theft of sensitive information

that can be exploited, etcetera. That's how it's looking at it. So again, as we reviewed before, it should also be a service that's key to the mission, and it's high value to the organization.

So best practice-- you've heard us mention this before-- we're going to say it again: To ensure that all participants have the same understanding, review all the information as the CIS begins. There may be additional people there that weren't part of those initial discussions. They may have happened a couple weeks ago and people's memory may not be the same.

Critical Service Information: Concepts and Terminology –2



An organization uses its assets to perform productive activities that enable it to provide operational services and accomplish its mission.

Best Practice

Throughout the survey, emphasize the selected critical service.

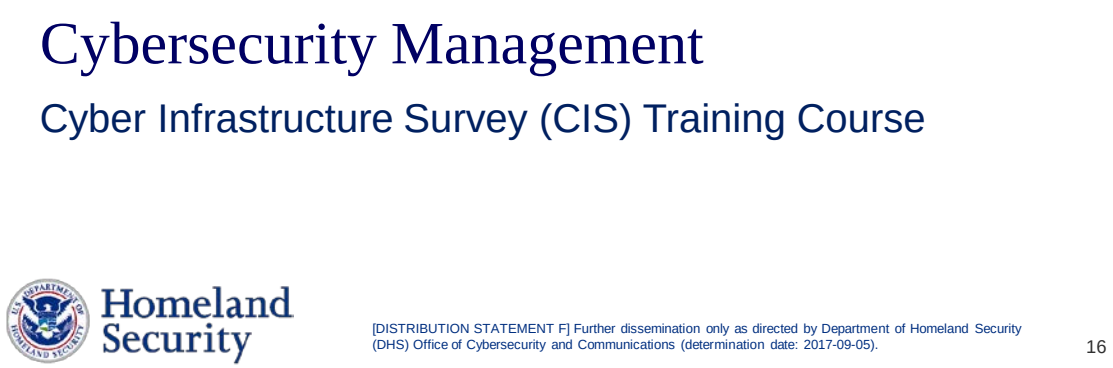
Homeland Security

15

**015 This is just a summary slide that you've seen before about the critical service. Take note of this best practice also. We've mentioned this before. As you're going through the assessment, you'll want to remind people that you are asking these questions in regards to the critical service only, and I'm sure for you guys that have done this a while you'll see when people drift; it'll become apparent when you need to do that.

Cybersecurity Management

Table of Contents



**016 So the next domain we're going to look at is cybersecurity management, and you'll start to see more of the QA aspects and other aspects that we've been talking about show up here.

Cybersecurity Management Domain –1

This part of the survey assesses the organization's administrative security controls and its program management capability. Specifically, it assesses

- the structure of leadership and management of the cybersecurity capability surrounding the critical service (CS),
- how the documentation of cybersecurity assets is managed,
- how updates and upgrades to cybersecurity assets are managed,
- the organization's adherence to a standard for assessing risk and implementing security controls, and
- the organization's documented security control plan and rules of behavior for personnel accessing its IT systems.

**017 This part of the survey assesses the organization's administrative security controls and its program management capability. Specifically, it's looking to assess the structure of the leadership and management of the cybersecurity capability surrounding this critical service provider; how the documentation of cybersecurity assets is managed; how updates and upgrades to the cybersecurity assets are managed; the organization's documented security control plan, etcetera. This is what this section is trying to get at.

Cybersecurity Management Domain –2

Cybersecurity Management Domain	Checkbox	If Yes	Text Input	Notes	Total
Cybersecurity Leadership	4	2		2	**8**
Cyber Service Architecture	3	9		6	**18**
Change Management	4			2	**6**
Lifecycle Tracking	6	2		2	**10**
Assessment and Evaluation	2	9		2	**13**
Cybersecurity Plan	2	6		2	**10**
Cybersecurity Exercises	1	6		2	**9**
Information Sharing	6	13		4	**23**
Total	**28**	**47**		**22**	**97**

This domain contains a total of **97** questions.

- There are 28 simple Checkbox responses.
- There are 47 If-Yes questions.
- There are 22 Notes questions.

Homeland Security

18

**018 Again, you've seen this, by the numbers. It's one of the largest domains, if not the largest, I think by a couple questions, and there's several subdomains to this section of the CIS.

Cybersecurity Leadership: Overview

Cybersecurity Management Domain	Checkbox	If Yes	Text Input	Notes	Total
Cybersecurity Leadership	4	2		2	**8**

In Cybersecurity Leadership, the goal is to assess the

- structure of the organization's cybersecurity leadership and
- use of third-party contractors or vendors in directly managing cybersecurity for the CS.

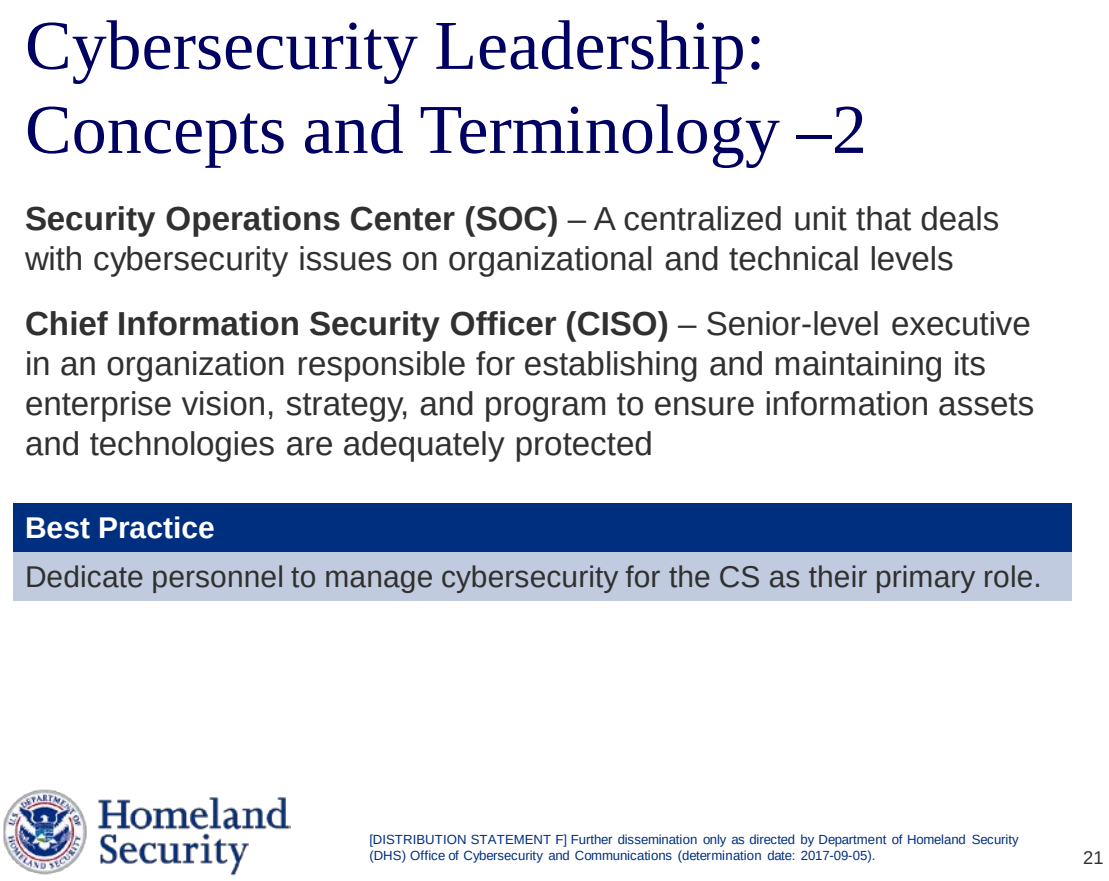
**019 So let's take the first one: Cybersecurity leadership. The goal is to assess the structure of the organization's cybersecurity leadership and use of third-party contractors or vendors involved in managing the cybersecurity of the critical service.

Cybersecurity Leadership: Concepts and Terminology –1

Third-Party Contract Management – Contracted cyber management or operational functions that are not done by the primary organization

Cyber Preparedness – The process of ensuring that an organization has developed, tested, and validated its capabilities to protect against, prevent, mitigate, respond to, and recover from a significant cyber incident

**020 Some terminology that you need to be aware of: third-party contract management, cyber preparedness-- I think these are obvious. If you have questions on these as we go through terminology, please speak up.



**021 Additional terminology: a security operations center, chief information security officer. I mean, the reason that these terms are being listed is because they're either in the Help as background or more primarily they're part of the questions themselves.

So a best practice that the CIS kind of hints at is to dedicate personnel to manage cybersecurity for the critical service itself. It should be their primary role. So as you're doing an assessment, this could be used even to start that conversation with the participant.

Cybersecurity Leadership: Training Tips –1

Possible Inconsistency – If Question 3.1 (Cybersecurity Management) is answered "Yes," check for consistencies with any specific organizational leaders and roles identified in Question 14.1 (Cybersecurity Forces). Similar checks are required for responses to Questions 3.2 through 3.4 (Cybersecurity Management).

Question 3.1 Is there a manager/department in charge of day-to-day cybersecurity management?	❑ No ☑ Yes

Homeland Security

**022 Let's look at some training tips in this area. A possible inconsistency that's seen-- and now we could use the companion guide that you all should have. You should have a small companion guide. Some of these are going to mention two different related questions. So like this one, as you can see, it's going to be looking at 3.1, which we show here, but also relating it to Question 14.1. So it would be a good idea to find 14.1 in your companion guide so you can look at that while we're looking at 3.1 here.

Let's go through the inconsistency. In Question 3.1, if that is answered

yes, check for consistency with any specific organizational leaders and roles in Question 14.1.

So Question 3.1: Is there a manager/department in charge of day-to-day cybersecurity management? Can I see the guide?

So 14.1 lists several types of roles. You would expect that if you're answering yes here, you wouldn't be answering "None of the above" there. That's a type of thing that they're looking for in the QA process.

Student: Well, okay now, Cybersecurity Policy and Planning Coordinator, Cybersecurity Training Official, Cybersecurity Incident Response Team Leader, Incident Commander, CERT, or None of the above. You may theoretically not have any of those.

Instructor: Yeah, that's true, but typically what they're expecting to see is if there's a manager or some person or department in charge of day-to-day cybersecurity that you would expect to see those roles, and that's what they're looking for, and if they truly don't, I would say put down that that's the answer, but I would make notes on that.

Student: I think the issue here is: Are the following positions formalized? Which leads me-- just from the outside looking in-- that these are positional titles they're looking for, which may not exist. You may have an ISSM that performs part

or some of these duties, or a CISO that may perform part or some of these duties, but not formally an individual in the position.

Instructor: So in the question, what they're asking for: Is there a manager or department in charge of day-to-day cybersecurity management? So I believe the thinking is if you're involved at a day-to-day level, that you would expect to see some of that.

Student: With questions like this are: Yes, and when you go through to the next questions they'll say, "You know, I don't have anybody by that title but I do have a person assigned to do a very similar role."

Instructor: Right, and then you would still select something there.

Student: Well, I think the keyword here though we're discussing is "formalized". To me, formalized means documented in a policy or procedure saying, "This person will hold this title and this role with this accountability and authority," and I'm with Ron on this one, is that I see this answered yes a lot but no to all of this stuff here. I see it more often than I see yes and yes.

Student: Yeah.

Instructor: What I can say is this is some of the items that they're looking for when they do QA, and if they're saying that they have active

management, day-to-day management of this-- cybersecurity management of the critical service, you would expect to see roles if they're doing something day to day as part of their position.

Instructor: But I think like said, the keyword is "formalized". Formalized implies that there's a piece of paper somewhere that has an assigned, "Here's this person's responsibilities by that job title," kind of a thing, and where I've had it, I've had people execute those responsibilities but it's a collateral duty. They have two people and they split them up or they...

Instructor: Yeah, this may be where you need to take notes to explain that.

Student: Yeah, because I've seen places where you have a one-man shop and he's the CISO, and so the CISO is in charge of day-to-day cybersecurity management, but the organization does not have an incident response policy, they don't have a training policy. So he's still in charge of day-to-day system but he's not going to have formalized any of these other roles. Yes, he's responsible for them, but it's never been formalized. So I can see that, yeah, the two questions are linked, but I wouldn't say that they're dependently linked.

Instructor: Right. So they might not always line up, but the idea is to look that if they're answering yes

here, when you get to that question you should be thinking about that, like is it really "No," is it really, "None of the above," and if it is, I would explain it in a comment.

Student: You're looking for inconsistencies.

Instructor: Exactly. Exactly. That's what they're looking for.

Student: No assessment is going to be a perfect fit for every place.

Instructor: Exactly.

Student: You just kind of got to roll with it.

Cybersecurity Leadership: Training Tips –2

Possible Inconsistency – If Question 3.2 (Cybersecurity Management) is answered "Yes" and the option "Operational/Functional" is checked as a specialized area, it is assumed that one or more cybersecurity positions should be checked in Question 14.1 (Cybersecurity Forces).

Question 3.2 Are there any other cybersecurity leaders with cyber responsibilities?	❑ No ☑ Yes If yes, where do they specialize? (*Check all that apply.)* ☑ Operational/functional ❑ Service ❑ Enterprise/governance ❑ Other _____

Homeland Security

**023 Instructor: So this is why I think this section is going to take the longest, because there's lots of discussion around these points. Notice also here the last sentence there.

Cybersecurity Leadership: Training Tips –1

Possible Inconsistency – If Question 3.1 (Cybersecurity Management) is answered "Yes," check for consistencies with any specific organizational leaders and roles identified in Question 14.1 (Cybersecurity Forces). Similar checks are required for responses to Questions 3.2 through 3.4 (Cybersecurity Management).

Question 3.1 Is there a manager/department in charge of day-to-day cybersecurity management?	❑ No ☑ Yes

Homeland Security

22

**022 Similar checks are required for responses to Question 3.2 through 3.4.

Cybersecurity Leadership: Training Tips –2

Possible Inconsistency – If Question 3.2 (Cybersecurity Management) is answered "Yes" and the option "Operational/Functional" is checked as a specialized area, it is assumed that one or more cybersecurity positions should be checked in Question 14.1 (Cybersecurity Forces).

Question 3.2 Are there any other cybersecurity leaders with cyber responsibilities?	❑ No ☑ Yes If yes, where do they specialize? (*Check all that apply.)* ☑ Operational/functional ❑ Service ❑ Enterprise/governance ❑ Other _____

Homeland Security

**023 So let's look at some of that. A possible inconsistency in Question 3.2: If Question 3.2 is answered yes and the option "Operational/functional" is checked--so Question 3.2: Are there any other cybersecurity leaders with cyber responsibilities? If you answer yes and then you say operational and functional leaders, it is assumed that one or more of the cybersecurity positions should be checked in 14.1, because you're saying, "I've got these people in place."

Student: See, I could see a security administrator or an ISM.

Student: That goes back to that "formalized" word.

Student: I think the application administrator, system administrator would be the one you're looking at here, but I would agree, this one links better to 14.1 than the previous one does.

Instructor: Yeah. So you need to have the understanding that we work with headquarters to receive a lot of the things that they're looking at and seeing in their QA checks. So this is bringing it to your attention so you have that link in your head and you can go back and try to make sure that you do have the right answer there. And as you said, sometimes maybe it is none, and you'd have to explain it.

Student: It may just be the titles. If they went with system administrator, network administrator, cybersecurity analyst, you'd probably get more checkmarks.

Student: I think it comes back to that "formalized" word. We need a better definition on formalized.

Student: Or just take it out completely. Are you looking for somebody who does the role? Is that what you're looking for? Or are you looking for the piece of paper that says somebody does--

Student: Or better yet, how about this: Would a position description be formal enough?

Student: Looking at Security Architect, a lot of places have a network architect, but they don't necessarily consider themselves the security architect. So what formalizes a security architect over a network architect? So yeah, my network architect does the security review. Is that good enough to formalize?

Instructor: In some organizations they truly may be the same person.

Student: Right. But you would think that they'd have to have it in his position description, saying, "Is responsible for security review on network architecture."

Student: Or the IRC or something.

Student: Yes. So the "formalized" word really is the hardest part about this whole thing for me.

Student: Did you guys write this? This one yours?

Instructor: So the survey-- we are teaching to what the survey is today. But these comments are good for us and it may effect change in the future.

Cybersecurity Leadership: Training Tips –3

Possible Inconsistency – As mentioned in the previous slide, if Question 3.2 (Cybersecurity Management) is answered "Yes" and the specialized area "Operational/Functional" is selected, answering "None of the above" to Question 14.1 (Cybersecurity Forces) would be inconsistent.

Question 14.1 Are the following positions formalized? (*Check all that apply.*)	Within your organization, ❑ Cybersecurity Policy and Planning Coordinator ❑ Cybersecurity Training Official ☑ None of the above Within the CCS environment, ❑ Cybersecurity Exercise Official ❑ Security Operations Personnel (i.e., Security Administrators, Security Analysts) ☑ None of the above

Homeland Security

**024 So, Tip 3. As mentioned in the previous slide, if Question 3.2 is answered yes and the specialized area "functional" is selected, answering "None of the above" to Question 14.1 would be inconsistent. So we're showing you the other part of that, and what we're trying to do is-- it's easier to follow along in your guide. When we have one up, you can see the other half of it. But many times we'll show you the other half as a second slide. But as we're moving along, it would be helpful to look up the question. There's an index in the front of the guide that tells you exactly where it's at. So what we did is we took out

everything that we're referencing in this section to make that small guide.

Student: Like this one, what I've seen-- like the Cybersecurity Training Official. I've seen where people go, "We have a training department that handles training across the organization. There's no one person that works cybersecurity specifically. It's a departmental function." Yes, there is somebody because you have a training manager. So I would check that as yes. I don't know if that's the intent that you're talking to now. I don't know if I should.

Instructor: I would say that if there's somebody really responsible for cybersecurity training, that would probably be...

Student: I'd say if their training program has a documented list saying that the training office handles all cybersecurity training, then yes, that's formalized and you could count that training manager as somebody.

Instructor: If it's just general training, then I wouldn't give that a yes.

Student: No, but I'm saying I've been to a place where they have a training department. They don't have one belly button in that department that specifically does cybersecurity training. They all did it, all three or four. It was a departmental function, not a subset of one person within that department.

Student: These don't have to be people. These can be departments.

Student: That's what I'm saying. They had a training--

Instructor: But somebody's responsible. That department's responsible for cybersecurity training. So, yeah.

Student: It was just one of many.

Instructor: So again, I would probably make the selection and then clarify it in notes. That way when they're doing QA they would see that hopefully.

Student: In fact, I've heard that more than any other type of response, is, "Don't have an exact person who does that, but our department does it overall," kind of a thing.

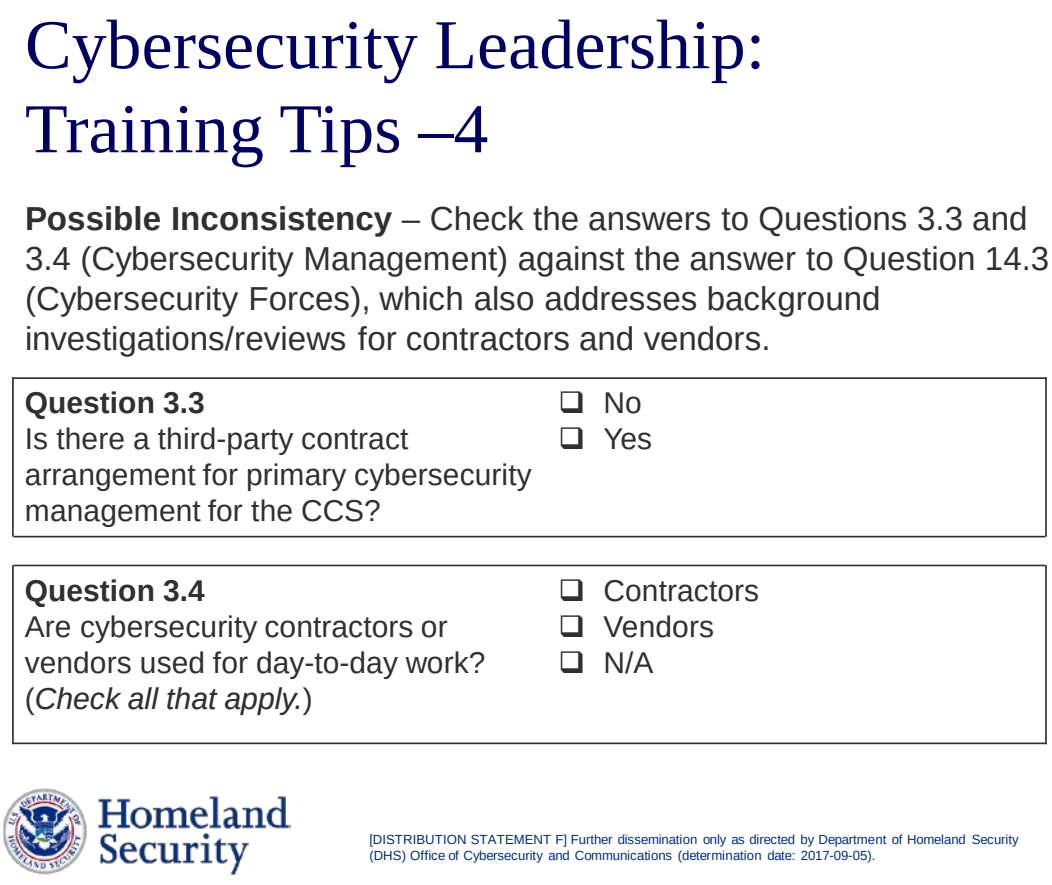
Student: As long as they have it written somewhere in that department's mission statement that they do handle security specifically, I would count it. If they don't-- if they just say, "Well, they handle any training that anybody throws at them," I wouldn't count that one.

Instructor: I would agree with that.

Student: I actually came across a division in Washington that has a training department but also has a cybersecurity training officer responsible to make sure that people

got their CEUs and keeps their certifications and stuff, and I thought, "That's pretty cool. That's what they're supposed to be doing."

Cybersecurity Leadership: Training Tips –4



**025 Instructor: Yeah. So let's look at Tip 4. Check the answers to Questions 3.3 and 3.4 against the answers to Question 14.3, which also address background investigations. So 3.3: Is there a third-party contract arrangement for the primary cybersecurity management of the CCS? In this case, the critical service. So one thing to note is we're using CS most of the time, but the tool still says CCS, Cyber Critical

Service. That's going to change. So we left it in the question to match what you would see in the tool. Are cybersecurity contractors or vendors use for day-to-day work?

Cybersecurity Leadership Training Tips –5

Cybersecurity Leadership Training Tips –5

Possible Inconsistency – As mentioned on the previous slide, the answers to Questions 3.3 and 3.4 (Cybersecurity Management) should be consistent with the answer to Question 14.3 (Cybersecurity Forces) as it relates to conducting background checks for contractors and vendors.

Question 14.3 Are background checks conducted for organizational and supporting personnel?	If applicable, contract cybersecurity personnel ❑ N/A ❑ No ❑ Yes If applicable, cybersecurity vendors ❑ N/A ❑ No ❑ Yes

Homeland Security

**026 So looking here at 14.3: Are background checks conducted for organizational and supporting personnel?

Cybersecurity Leadership: Training Tips –4

Possible Inconsistency – Check the answers to Questions 3.3 and 3.4 (Cybersecurity Management) against the answer to Question 14.3 (Cybersecurity Forces), which also addresses background investigations/reviews for contractors and vendors.

Question 3.3 Is there a third-party contract arrangement for primary cybersecurity management for the CCS?	❑ No ❑ Yes

Question 3.4 Are cybersecurity contractors or vendors used for day-to-day work? (*Check all that apply.*)	❑ Contractors ❑ Vendors ❑ N/A

Homeland Security

25

**025 So back at 3.3 and 3.4, if you're indicating that you do have vendors and contractors, you shouldn't be putting this here as Not Applicable.

Cybersecurity Leadership Training Tips –5

Possible Inconsistency – As mentioned on the previous slide, the answers to Questions 3.3 and 3.4 (Cybersecurity Management) should be consistent with the answer to Question 14.3 (Cybersecurity Forces) as it relates to conducting background checks for contractors and vendors.

Question 14.3 Are background checks conducted for organizational and supporting personnel?	If applicable, contract cybersecurity personnel ❑ N/A ❑ No ❑ Yes If applicable, cybersecurity vendors ❑ N/A ❑ No ❑ Yes

Homeland Security

**026 You should be answers yes or no to the question itself that relate to them. So even when you're here at 14.3, you kind of got to remember, "Hey, is that consistent with maybe what we already had?"

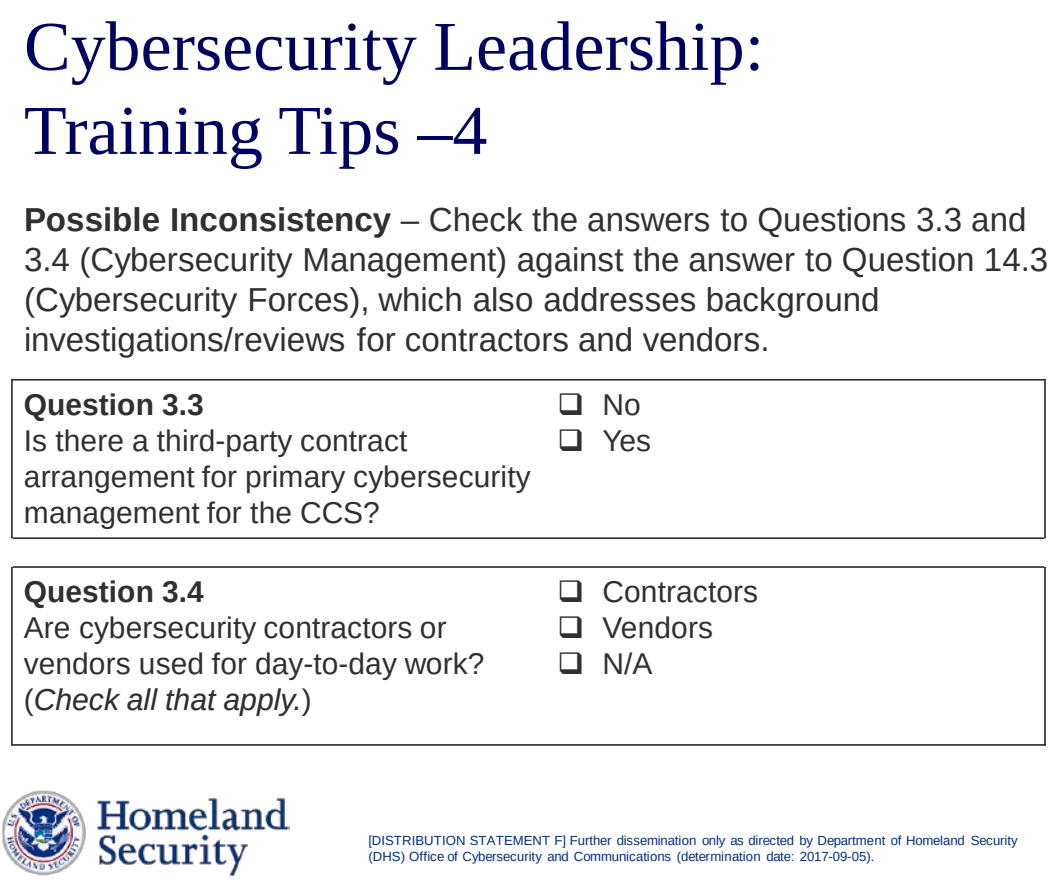
Student: So you could Not Applicable for one, but you couldn't put it for both then.

Instructor: Well no, I don't think you should. So if applicable, contract cybersecurity personnel-- if I say--

Student: Because if they're using contract cybersecurity personnel but

they're not using vendors-- so the first question, it says "Or."

Cybersecurity Leadership: Training Tips –4



**025 And then when you get down to 14.3, it separates them into two separate ones. So one could be N/A but both of them can't be N/A.

Instructor: Right.

Cyber Service Architecture: Overview

Cybersecurity Management Domain	Checkbox	If Yes	Text Input	Notes	Total
Cyber Service Architecture	3	9		6	**18**

In Cyber Service Architecture, the goal is to assess the

- effort to inventory and document the organization's critical service assets,
- effort to map cyber assets and the associated network infrastructure to provide a comprehensive logical overview of the enterprise architecture, and
- management and currency of all documentation.

**027 So we're going to go into the next portion of that domain. We're going to go into the next subdomain here, which is cybersecurity architecture. So the goal here is to assess the effort to inventory and document the organization's critical assets, the effort to map cyber assets and the associated network infrastructure, etcetera, and management and currency of all documentation.

Cyber Service Architecture: Concepts and Terminology –1

System Architecture – Documentation providing a conceptual layout of the critical service's network, consisting of the hardware, software, connectivity, communication protocols, and mode of transmission, such as wired or wireless

Security Architecture – Documentation providing a conceptual layout that describes how the security controls are positioned and how they relate to the overall systems architecture

Network Map – Documentation providing a visual representation of the system architecture and security architecture (sometimes referred to as a network topology map)

**028 Terminology for this section. A system architecture, security architecture-- these are things you should be familiar with. Those two are not one and the same. Security architecture: Documentation providing a conceptual layout that describes how the security controls are positioned and how they relate to the overall system architecture. Network map I'm sure everybody's familiar with.

Cyber Service Architecture: Concepts and Terminology –2

Critical Cyber Assets – Hardware, software, firmware, or personnel that is directly associated with an organization's necessary services, that—if destroyed, degraded, or otherwise rendered unavailable—would affect the reliability or operability of the CS

Best Practice

Document system and security architectures that IT and cybersecurity personnel can use. Update these documents regularly and mandate a process for signoffs.

Homeland Security

**029 Critical cyber assets: Hardware, software, firmware or personnel that is directly associated with your organization's services that if destroyed, degraded and so on would render it unavailable-- so if you recall our discussion around a critical service and the assets that make it up.

So a best practice, like an organizational best practice in this area: Document systems and security architectures that IT and cybersecurity personnel can use. Update these documents regularly and mandate a process for signoffs. These type of documents should be controlled like any other.

Student: I think it's funny the number of times I've gone in, when you're starting the assessment with them and you're saying, "Do you have network diagrams that we can use to help you scope?" and they start saying, "Well, they're a little old," and stuff like that, but then when you get to this question and you're like, "Do you guys have current network diagrams?", they're like, "Oh yeah, yeah, we have those. We keep them updated." It's like, "We just talked about this at the beginning of the assessment."

Instructor: Right. So that's what this section is really trying to get to.

Change Management: Overview

Cybersecurity Management Domain	Checkbox	If Yes	Text Input	Notes	Total
Change Management	4			2	**6**

In Change Management, the goal is to assess the organization's policies and procedures required to change the baseline configuration of cybersecurity controls for the CS.

**030 Moving on to the next subdomain, Change Management. The goal here is to assess the organization's policies and procedures required to change the baseline configuration of cybersecurity controls for the critical service.

Change Management: Concepts and Terminology –1

Security Baseline – A set of specifications for hardware, firmware, software, or a service that has been formally reviewed and agreed upon at a given point in time and should only be changed through a formal change procedure

Example
A firewall's configuration could allow **agreed-upon** port numbers and block all others.

Change Management – Formal control procedures required to change the baseline configuration of hardware, firmware, software, or a service

**031 Terminology. Security baseline: A set of specifications for hardware, firmware, software, etcetera, upon a given point in time and should only be changed through a formal change procedure.

So an example: You have firewall configuration. Typically that's very well controlled and the changes are agreed to. In fact, most of the changes around that should be going through your standard change control aspects. Change management is a formal controlled procedure around change.

Change Management: Concepts and Terminology –2

Revision Logs – A detailed history of all changes made to hardware, firmware, software, or a service as required by a change management program (A revision log allows anyone to review detailed change history at a later date.)

Ad Hoc – The absence of formal or documented processes, procedures, or guidelines

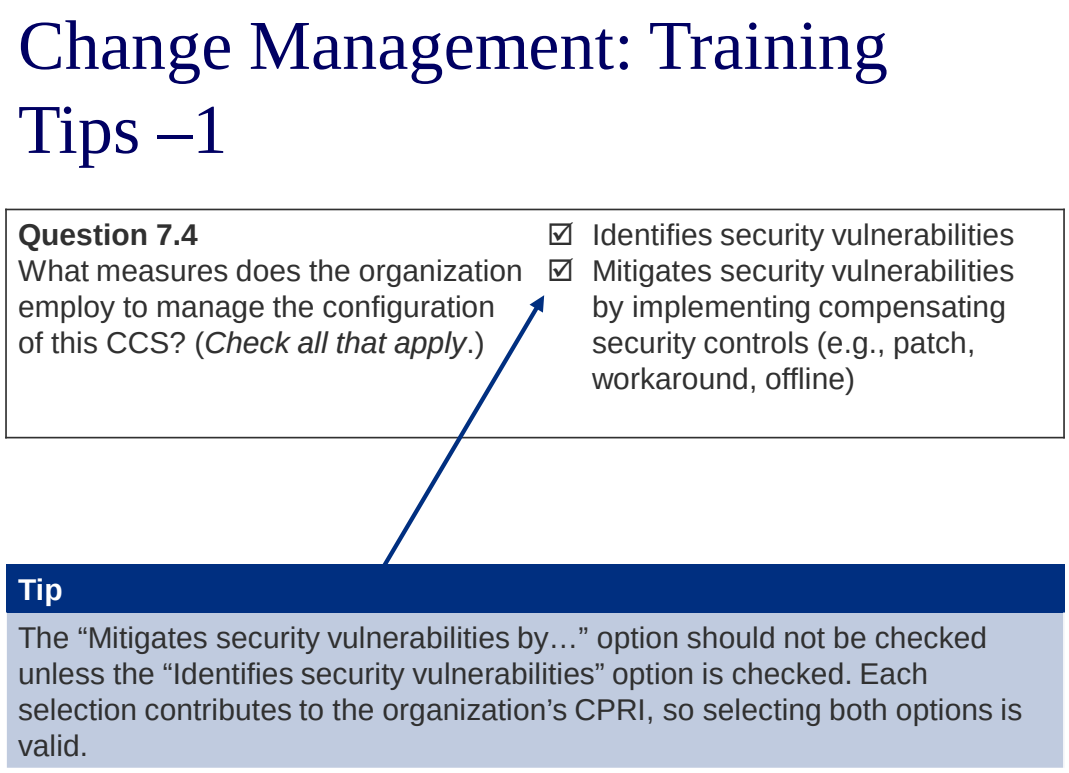
Best Practice

Maintain the integrity of cyber assets by using a change management program that dictates the procedures and documentation required before any change can be made to network resources, plans, architecture, etc.

Homeland Security

**032 Revision logs and ad hoc. I think those terms are pretty understandable, but those are terminology that come up in this section.

So an organization best practice: Maintain the integrity of cyber assets by using change management program that dictates the procedures and documentation required before any changes can be made.



**033 So let's look at some of the training tips in this section. So, Question 7.4: What measures does the organization employ to manage the configuration of the CCS, of the critical service? And notice that both of those are checked, "Identifies security vulnerabilities" and "Mitigates security vulnerabilities".

So looking at the tip, "The tip mitigates security vulnerability by..." option should not be checked unless the "identifies security vulnerabilities" option is checked. Each selection contributes to the organization's CPRI, so selecting both is valid.

So what we're trying to say there is when we first say this question, I looked at this and said, "I might say I select mitigates because to me that includes identifying. I'm not going to mitigate something if I haven't identified it." But the right thing to do here is to actually select both because many times in the CIS both of these incrementally contribute to the CPRI itself. So if you didn't do that, you've actually shortchanged the score for the participant.

Student: I know your goal is not for us to pick apart every question you use as an example, but I had a place where they said they had Windows Update checked by default. They don't identify any vulnerabilities, they just patch automatically without-- it's not under control. It just happens.

Student: I also see a lot of places like to answer this, "No, we're not scanning for vulnerabilities. We don't have a network vulnerability scanner. We're not identifying our vulnerabilities by network scans, but yes, we have a mitigation strategy: to apply patches as patches come in."

Instructor: So I see what you're saying. So I would say is that really the entire environment? So in this case, if they're not identifying, then I probably would leave it blank. But what we're trying to bring to your attention, if they say they're doing mitigation, it is worth asking about the identification, because don't assume that mitigation covers that,

because otherwise the score's not accurate.

Student: I'm just going off that, where it says, "Option should not be checked unless the 'identifies security vulnerabilities' option is checked." I have seen several places where I've checked the mitigates but did not check the identifies.

Student: Yeah, they don't do any active-- they're not actually looking for any vulnerabilities.

Instructor: So that's probably we should take a note on and look at rephrasing.

Student: Yeah, because it's a backwards way of doing--

Student: They just don't have the people or time. They'll patch automatically.

Student: Right, so they're going to patch automatically something that they may not need to patch, but--

Student: They'd rather do that than not patch at all.

Student: Yeah.

Student: That's odd. Okay.

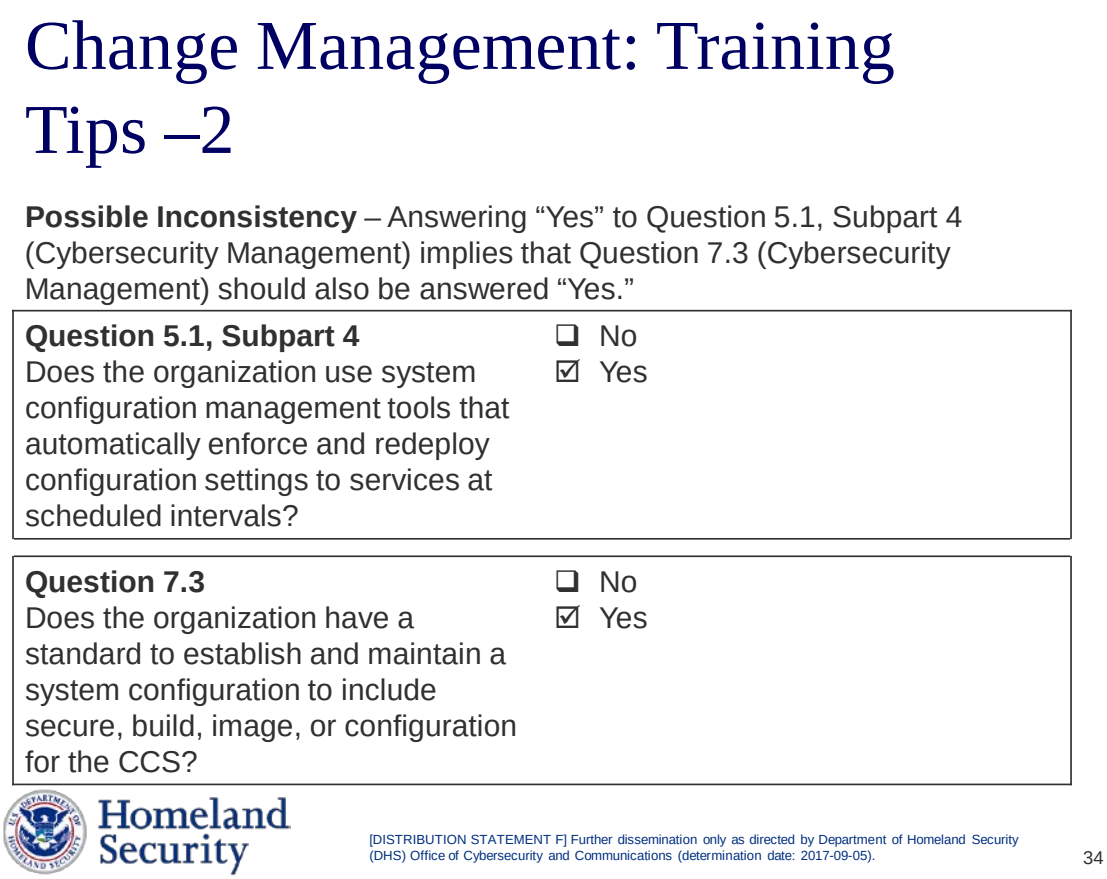
Student: You're going to see some weird stuff, man, I'm telling you.

Student: I mean, I can see the argument there that they're not really mitigating security vulnerability;

they're having a patch management program. But they're not mitigating security vulnerabilities, they're just patching.

Student: Because they don't know what vulnerabilities they have.

Student: Yeah, they don't know what vulnerabilities they have. So I could see that argument too, that we should leave both boxes unchecked at that point because their patch management process is not a security-- it's not a vulnerability mitigation process. So.



**034 Student: But what were you going to do? What do you guys want to do? So let's be consistent.

Student: I don't think you can answer that without being very specific to the person, and asking some additional questions to figure it out.

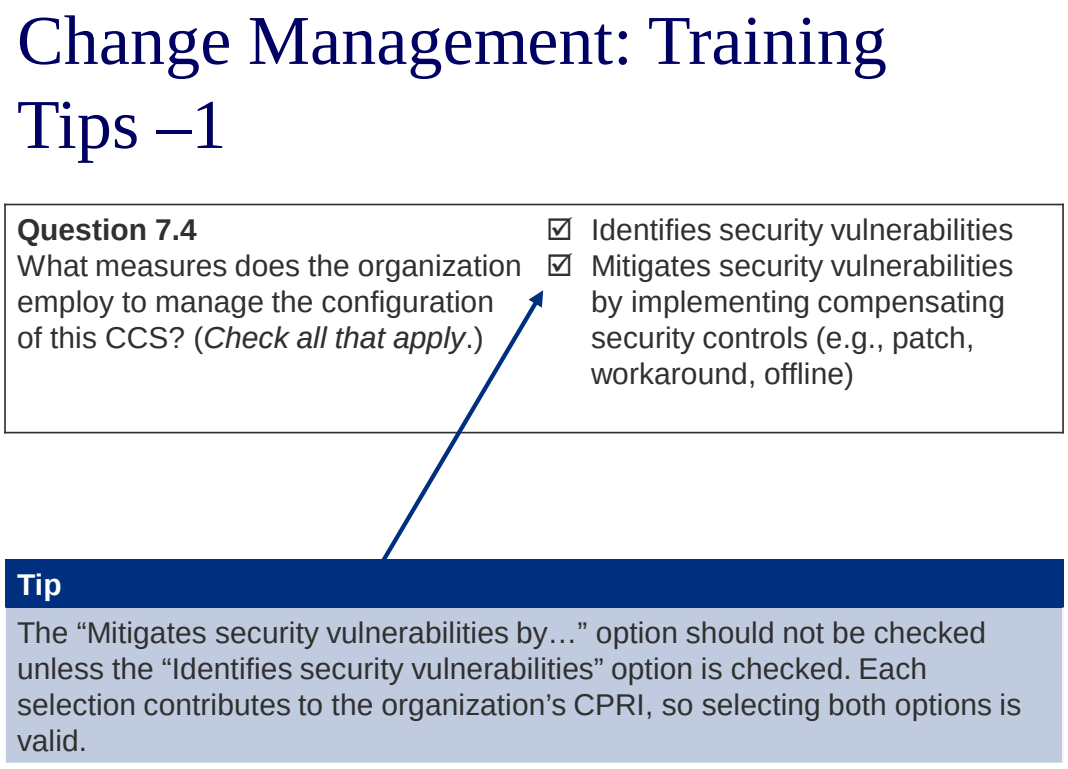
Student: I guess going back to what Phil was saying, just put it in your notes if you feel that strongly.

Instructor: Yeah, so this is where when you're doing assessments you're hearing answers and you're going to do a little bit more digging

to understand the real situation, and that's going to be across the board.

Student: So what do you think? On a question like that-- now, this is my-

Change Management: Training Tips –1



**033 Instructor: This one?

Student: Yeah, like this, where your stakeholder says, "I want you to check that yes," and your gut feeling is, "You know what?"-- just like Clint said, I personally don't think you have any sort of a process for mitigating vulnerabilities; you're just doing something by default. I'm going to check that yes because my

stakeholder told me to check it yes. It's ultimately up to them, right?

Instructor: No. What we do, you're soliciting input from them but you are the assessor, so you should be putting down what you believe the most accurate answer is. Now, you may tell them that, "I'm going to put a note here in the comments to describe the situation," but typically if I'm on a different type of assessment, say, and I'm hearing answers one way and they're saying it another, I'm going to say, "This is what I believe it is, this is why," and we're responsible for putting down the most accurate answer, whether they always agree or not. Now, I try to come to agreement with them, but sometimes that doesn't always work, but I'll explain why that is. And in this case, you have the ability to put those comments in to maybe better explain the situation so it shows up differently in what they see on the dashboard.

Student: I guess my response to a situation like that-- which I see where the pressure to put. My question to them is: If you don't know what your security vulnerabilities are, how do you know that you're mitigating them?

Student: It's not so much a deal on the CRR because you're not projecting the answers. Here you--

Instructor: Yeah, but even there, like when we're going through it, I'm saying, "This is what I believe I'm

hearing from everybody here. This is what I believe it is." And if they want to challenge that, I would say, "Please explain it. Convince me," and if not, I'm going to say, "This is what I'm going to record because I believe this is what's being described," and you will have a chance to review it once you get it to make any changes, and that discussion can be had then as well.

Student: Or they create their own scenario or they answer it the way they thought it should be.

Instructor: Right.

Student: I did have a customer that we went down to do a CIS with them and the chief technology officer was there and he wanted the assessment to show how far the program had come. He was expecting everything to be yeses and everything, so he wanted to use the dashboard as a model to show upper management what he had done in his tenure for the last year he was there. At about halfway through the assessment he stormed out of the room upset because we would not answer the questions the way that he wanted. We would say, "We're hearing this," and we kept answering that way. The rest of his group was excited about the answers we were actually giving. So the people who were actually going to have to make changes and understood the security implications, they knew how much farther they needed to go and they were happy with it, but we did lose

him for the rest of the day because he was upset that we wouldn't answer the questions "yes" when he wanted them "yes".

Instructor: I really try to explain in those situations that this is for the organization's benefit. "We're not using it. It's your data. You should want to accurate baseline of where you truly are."

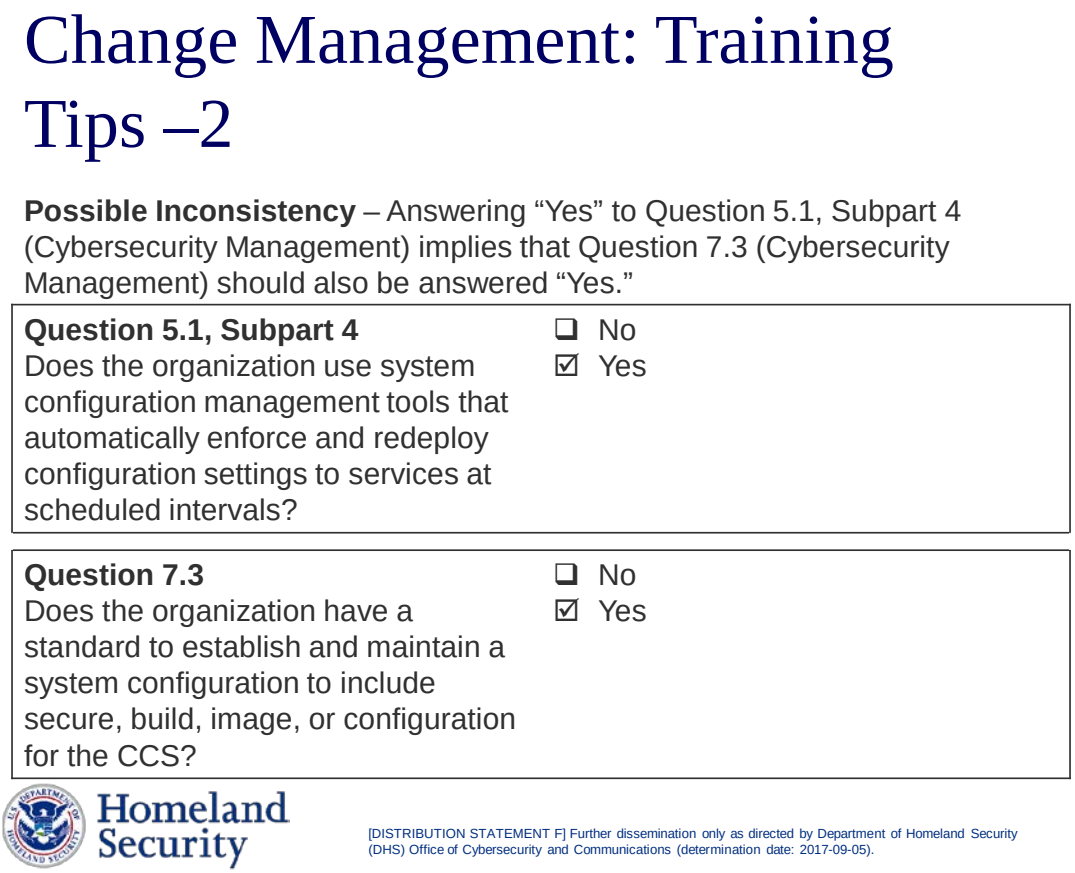
Student: Unless somebody's trying to improve their...

Instructor: Yeah. So normally though most people in the room understand that. Once in a while you run into situations like that of it's going to be what it's going to be. I've also had the opposite where I've had somebody in management say, "These guys are thinking about this correctly. We are not always looking at what service and how we're affecting it and how to answer these kind of questions. Let's all be honest and get a good baseline." I've seen both ends of the spectrum.

Student: My customer ended up apologizing. He called us and apologized later, saying that he was just expecting his program to score a lot higher and he thanked us and said that this was much more valuable, and he said that it just took him a little while because he really thought that he was farther along than what he was. We shed a new light on his entire organization that he never saw before. We brought to bear vulnerabilities that he didn't know existed.

Instructor: Exactly. It's not always easy.

Change Management: Training Tips –2



**034 So let's look at an additional tip. So answering yes to Question 5.1 subpart 4 implies that Question 7.3, if you want to look in your guide, should also be answered yes. So realize that what we're showing here may not always show all the options that are in the guide. So Question 5.1 subpart 4: Does the organization use system configuration management tools that automatically enforce and redeploy configuration settings? Question 7.3: Does the organization have a standard to

establish and maintain system configuration, to include secure build image or configuration for the CCS?

So if they have tools that are doing it, you would expect this to be a yes here. And so--

Student: I have a common issue with that though, that we're supposed to be using the least denominator. So yes, they do have a tool-- let's say that they're using a version of active directory or something that automatically redeploys. So yes, they have a configuration management tool that automatically enforces, but they only have the standard to do system configurations for their Windows boxes, not their Linux, not their-- so would you answer no to both of those areas then?

Instructor: Correct.

Student: So unless Question 5.1 covers everything in the organization-

Instructor: Covers this service, not the organization.

Student: Or I'm sorry, their service.

Instructor: Correct. Yes. So if that's--

Student: So just because they have one thing that does it, but if it doesn't cover everything that's part of that, we should be marking that no, with just the caveat that they have this for Windows but they're

lacking in Linux and lacking in firewalls.

Instructor: You'd put that in the comments. Yep. Right.

Student: The scope is a service.

Instructor: The scope is the service. So to his point, if part of my service is Windows and it's happening there, but I also have network, I also have Linux, and maybe it's even happening on the network side but really not on the Linux side, then you're supposed to be putting down the weakest--

Student: Or if I had a Windows desktop against a Unix server farm in the service.

Instructor: Well, depends on the service, right?

Student: Right. What I'm saying is you may find that the GPOs are on all the desktops running that, but the Unix boxes are in a complete separate organization.

Instructor: That's kind of the point, right?

Student: And so, yeah.

Instructor: But even so, if they are, the person that hopefully is-- one or two people doing this hopefully have that background to answer it.

Student: Or their CCB should be taking care of most of that.

Student: That's why scoping in the very beginning, when you're going through what makes up this system--

Instructor: Becomes important.

Student: --I'm always really careful on what actual operating systems, what network devices are you actually using. Because when I ask a lot of these questions, like, "Do you do it for this?", I go back to that first page and say, "You do it for each one of these components."

Instructor: Yep. Right.

Student: I think I might have been scoring wrong on that, because if they had some that covered a good portion of it I was answering yes, and now I know that I need to answer-- if it's not yes across everything then I need to go to no.

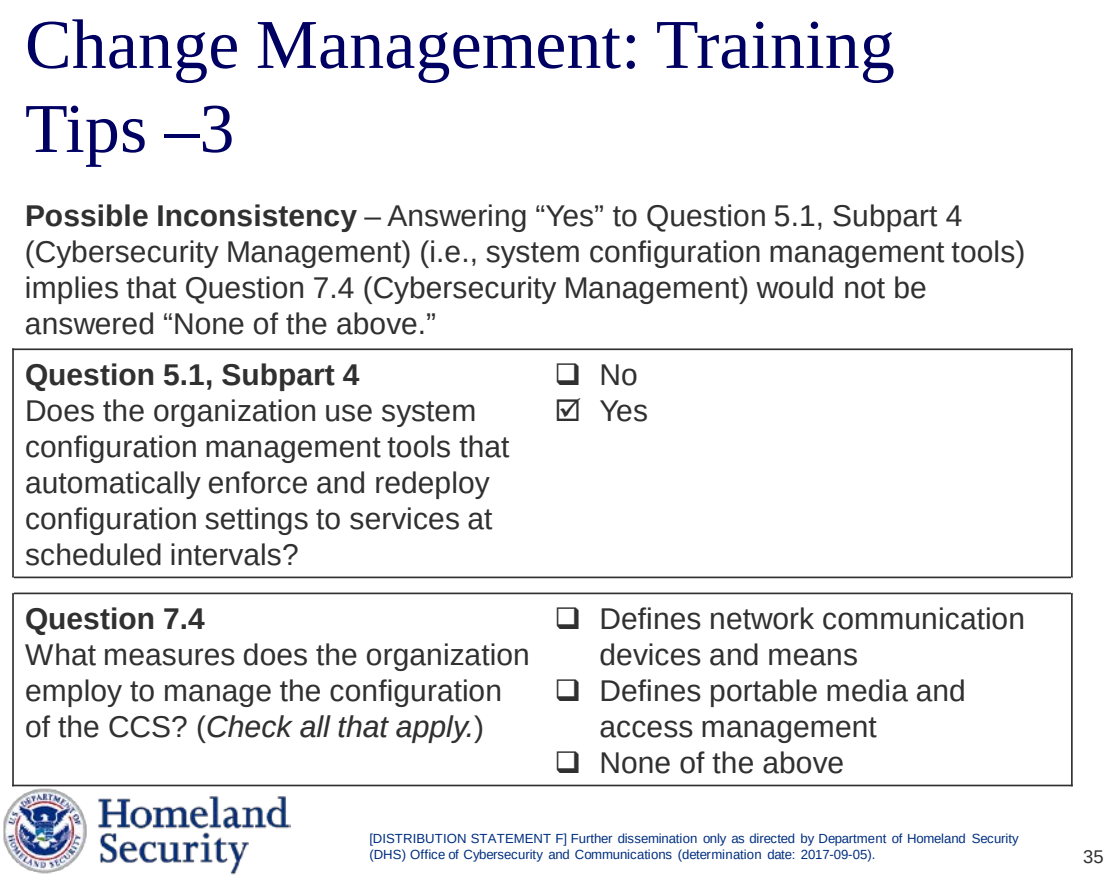
Student: So it's an all or nothing.

Instructor: Yeah, you're looking for, again, that least common-- that least effective implementation. And so you're making judgment calls on a lot of this too, because even as you're describing that service, I'm going to be looking at the major components of that service. I may not care about smaller closets, but I may care about a closet that feeds other ones. I may not care that the one with only 20 things on it-- it just kind of depends. So you're going to have to kind of feel it out as you do that.

Wow, this discussion has caused me to kind of lose where I'm at here. Okay.

Student: Next slide.

Change Management: Training Tips –3



**035 Instructor: Yes, thank you. Okay, so Tip 3 here: Answering yes to Question 5.1 subpart 4 implies that Question 7.4 would not be answered "None of the above." So Question 5.1 subpart 4: Does the organization use system configuration management tools to automatically enforce and redeploy configuration settings, etcetera? Question 7.4: What measures does the organization

employ to manage the configuration of the CCS? Defines network communications, defines portable media, etcetera. You would think you would not have "None of the above" here.

Student: It depends on what they mean by network communication devices. I mean, are they talking about desktops? Laptops? Tablets? Are they talking about switches/routers? I mean--

Student: I would think they'd be going with switches and routers since endpoints would be your--

Instructor: Yeah, and there's a separate part about endpoints.

Student: This is strictly endpoints?

Instructor: There's separate questions on endpoints throughout here.

Student: So you've got your switches and routers. So are you using something that controls that configuration?

Instructor: Yep. You would expect that if they have this-- this is just an inconsistency they're looking for. Again, I think this is one of those situations where if it's truly that they don't, you might need to explain the selection.

Student: This is where you need the little blue bubble to click on and say, "What exactly are they looking for here?"

Change Management: Training Tips –4

Possible Inconsistency – Answering Question 7.3 (Cybersecurity Management) "Yes" implies that Question 7.4 (Cybersecurity Management) would not be answered "None of the above."

Question 7.3 Does the organization have a standard to establish and maintain a system configuration to include secure, build, image, or configuration for the CCS?	❑ No ☑ Yes

Question 7.4 What measures does the organization employ to manage the configuration of the CCS? (*Check all that apply*.)	❑ Defines network communication devices and means ❑ Defines portable media and access management ❑ None of the above

Homeland Security

36

**036 Instructor: So Tip 4 in this area: Answering Question 7.3 yes implies that Question 7.4 would not be answered "None of the above". So again, 7.3: Does the organization have a standard to establish and maintain, etcetera? Question 7.4: What measures does the organization employ-- did we just do this same one?

Student: No. That one actually-- that one I could see fitting those two definitions. The last one was the more tricky.

Instructor: Right. So what measures does the organization

employ to manage the configuration of the CCS? Defines network communications--

Instructor: Yep.

Student: I can see an organization having a standard that they haven't implemented yet, but that would be rare. That would be really rare. Like you caught them at just the right moment where, "We've defined and have the standard, but..."

Instructor: And that could happen. They might be just completing the definition and they haven't really-- so that would be something you would have to explain.

Lifecycle Tracking: Overview

Cybersecurity Management Domain	Checkbox	If Yes	Text Input	Notes	Total
Lifecycle Tracking	6	2		2	**10**

In Lifecycle Tracking, the goal is to assess how the organization manages CS assets throughout their lifecycle.

**037 I'm not sure why you started laughing, but that's okay.

Student: Well, because this is the bane of my existence, but go ahead.

Student: Not any more.

Student: Yeah, that's true. Sorry. I'm in a new place. I can sit back and laugh.

Instructor: Let's look at the live cycle tracking subdomain.

Lifecycle Tracking: Concepts and Terminology –1

Lifecycle Management – The process of managing the entire lifecycle of an information technology asset, from inception through engineering design and manufacture, to service and disposal

Patch Management – An area of lifecycle management that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system (This capability is critical to keeping systems updated against critical vulnerabilities.)

**038 So, some terminology. Lifecycle management, patch management-- I believe people are familiar with these terms, right? These are directly addressed in this section.

Lifecycle Tracking: Concepts and Terminology –2

Third-Party Vendor – Any entity outside the organization that provides a service or product to the organization

Critical Vulnerability – A security flaw or weakness in a cyber system that can be exploited by an attacker to severely impact the CS

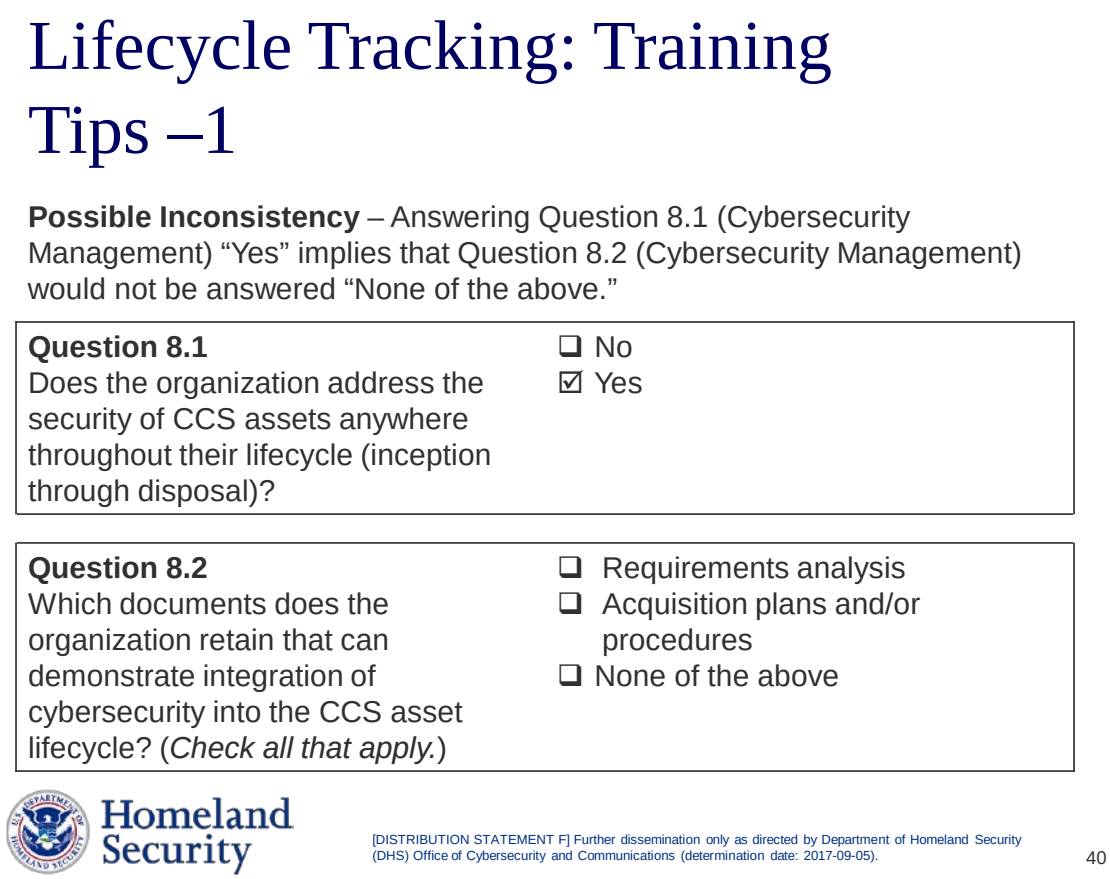
Best Practice

Enforce standards and requirements as part of lifecycle management before putting CS assets into service.

Homeland Security

**039 Third-party vendor. Critical vulnerability: A security flaw or weakness in a cyber system that can be exploited by an attacker. This is not a threat; this is a vulnerability.

Kind of an organization best practice: Enforce standards and requirements as part of a lifecycle management before putting CS assets into service.



**040 So let's look at some of the training tips in this area. Again, a possible inconsistency. So answering Question 8.1 yes implies that Question 8.2 would not be answered "None of the above". Does the organization address the security of the critical service assets anywhere throughout the lifecycle, inception through disposal? Which documents does the organization retain that can demonstrate integration of cybersecurity into the asset lifecycle? So if you're saying you do that, you would expect to have some sort of documentation that kind of shows that you are doing that. You wouldn't expect to see a "None of the

above" here. That's the intent. Not to say that maybe they don't have these particular ones, but you would expect that if they are they would have some kind of requirements analysis, right?

Student: Right, right.

Student: I would think that would be a question they would-- and this isn't something for you-- but that they would just make Question 8.2 a dropdown when you selected Yes for 8.1.

Student: Right.

Instructor: Yeah. And so that also goes along with-- and I'm not the one to say that it's not-- I don't use the assessment that often, but it also plays into the tip we gave earlier where it really is beneficial to maybe click on the Yes answer to make sure there isn't additional information there that you can then show an organization. So if that were the case that it was a drop-down, you'd be probably clicking there, and maybe that makes more logical sense, Clint. I'm not certain.

Lifecycle Tracking: Training Tips –2

Possible Inconsistency – Remind participants that the term *critical vulnerability* in Question 8.5 (Cybersecurity Management) refers to the participant's definition of that term and not a vendor's definition.

Question 8.5 Approximately what percentage of CCS systems is not or cannot be updated with respect to critical vulnerabilities? (e.g., legacy system or business reason - i.e., break software application)	❑ 75% or more ❑ Greater than or equal to 50% but less than 75% ❑ Greater than or equal to 25% but less than 50% ❑ Greater than or equal to 10% but less than 25% ❑ Less than 10%

**041 So Tip 2 in this area: Remind participants that the term "critical vulnerability" in Question 8.5 refers to the participant's definition of that term and not the vendor's. And this is important, because Microsoft may say it's critical, but in my environment, I may not agree with them, and it may not be the same definition as the vendor.

Student: If you keep running those Windows NT servers then we'll just...

Instructor: Okay. So, the point being though when they're answering this question, it's really their definition, not necessarily the vendor.

Now, in most instances, like you're saying, they may just accept the vendor and say, "We're going to patch everything critical anyway." But it's meant to be their definition, because if they-- to your point earlier-- if they're doing that evaluation and understanding and identifying their vulnerabilities, they're going to analyze which ones really pertain to their environment.

Student: Yeah, but that's way outside the standard. I mean, I was being facetious about Windows NT servers, but right now you're running into end-of-life for Windows 2003 servers. Windows 2008s are supposed to end-of-life and stop support next year. So when does a critical vulnerability become a critical vulnerability?

Student: When it shuts your service down.

Student: Well, I mean, okay, but if it doesn't shut your service down but it's highly vulnerable--

Instructor: I think you're taking this way beyond where it needs to be.

Student: Well, I'm looking at it from a cybersecurity perspective.

Instructor: So am I. So if I'm in an environment and I see a vulnerability and I'm looking at how we implement this system, I may not agree in that in my particular environment, just Microsoft called it critical that I'm

going to say it's critical. We're doing that evaluation and it may be a lesser value that I choose to give it.

Student: But if you can't patch it anymore because patches are no longer being supplied for your--

Instructor: But again, you're way beyond the point. All we're saying here is it should be their understanding of what's critical in their environment. I'm not arguing the fact that if it can't be patched that doesn't represent something critical, but in this instance, they should be applying their definition, is what it is, not the vendors.

Student: So to give you an example, we had a customer-- this came up on this particular question-- in which they had a web server that the web server was only stood up for communication between them and the Department of Revenue. It was really well segmented off, but there was what Microsoft called a critical vulnerability on the server. They did not consider it critical because there's only limited access to that server. It was an internal server to them, not outward, public-facing or anything like that, and if they patched it with the critical vulnerability it would break the software that was running on it. So they couldn't patch it, but they didn't consider it critical because it was not open or accessible by the internet.

Instructor: Right. The other mitigations they put in place.

Student: Right. To them it was not a critical vulnerability, so they did not consider that as something that couldn't be patched.

Instructor: Right. What we're trying to point out here is how to correctly think about the question intent.

Assessment and Evaluation: Overview

Assessment and Evaluation: Overview

Cybersecurity Management Domain	Checkbox	If Yes	Text Input	Notes	Total
Assessment and Evaluation	2	9		2	**13**

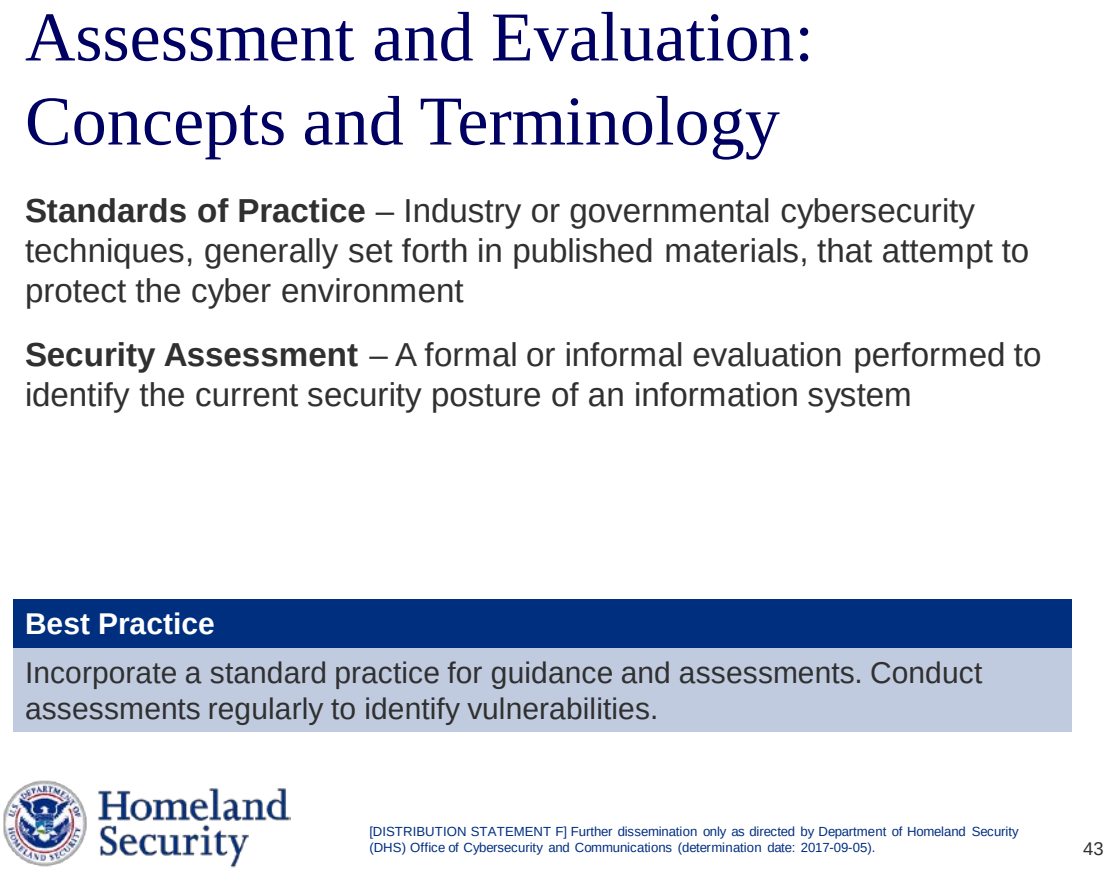
In Assessment and Evaluation, the goal is to assess if and how the organization evaluates the cybersecurity practices it has implemented in support of the CS.

**042 Student: And their risk appetite might be different from the standard.

Instructor: Exactly. Yep. So let's move on to the next subarea: Assessment and evaluation. The goal

is to assess if and how the organization evaluates their cybersecurity practices.

Assessment and Evaluation: Concepts and Terminology



**043 Terminology in this area. Standards of practice, security assessment. A best practice: Incorporate a standard practice for guidance and assessments. Conduct assessments regularly to identify vulnerabilities.

Assessment and Evaluation: Training Tips

Training Tip – Question 9.2, Subpart 2 (Cybersecurity Management) addresses the frequency with which a task is performed, while Subpart 3 describes the tasks that may be performed. Allow the participant to select from the list in Subpart 3 before selecting a frequency in Subpart 2.

Question 9.2, Subpart 3	
In what ways are the CCS assets assessed? (*Check all that apply.*)	❑ Internal vulnerability testing ❑ External vulnerability testing ❑ Internal penetration testing ❑ External penetration testing ❑ Documentation review (tabletop) ❑ Manual checklist ❑ None of the above

Homeland Security

**044 Some of the tips in this area. Question 9.2, subpart 2: Address the frequency with which a task is performed, while subpart 3 describes a task that may be performed. So allowing the participant to select from the list in subpart 3 before selecting the frequency makes it easier for the participant to think about the frequency they're doing something.

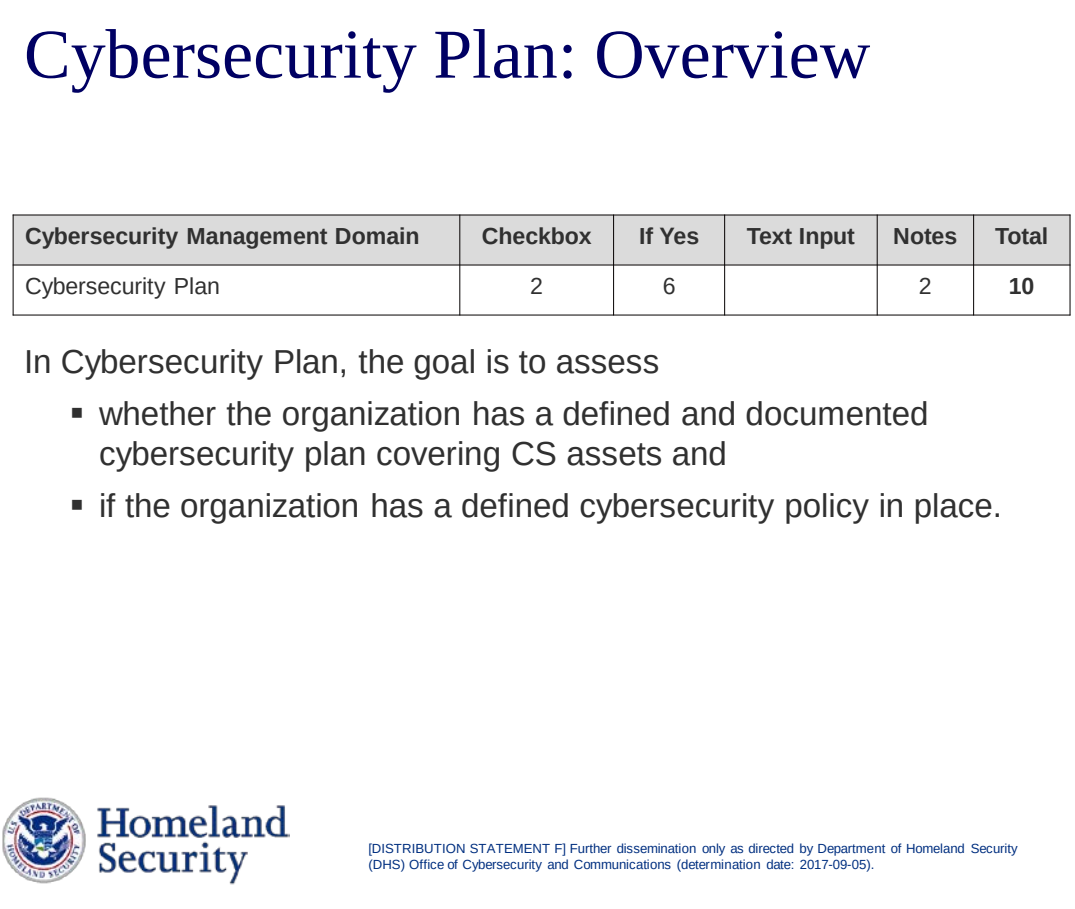
So this could happen a couple different ways in the CIS, so we're kind of suggesting as a common practice that when you see a situation like this, sometimes it's beneficial to move ahead to a different subpart, then go back and

talk about the frequency with which those things are being done, because now they have in their mind, "Okay, we do the first three and here's the frequency we do them," versus asking frequency first and they're not sure what you're really asking about. So it's just kind of a tip on how to approach it.

Questions? Good.

Student: That actually makes sense.

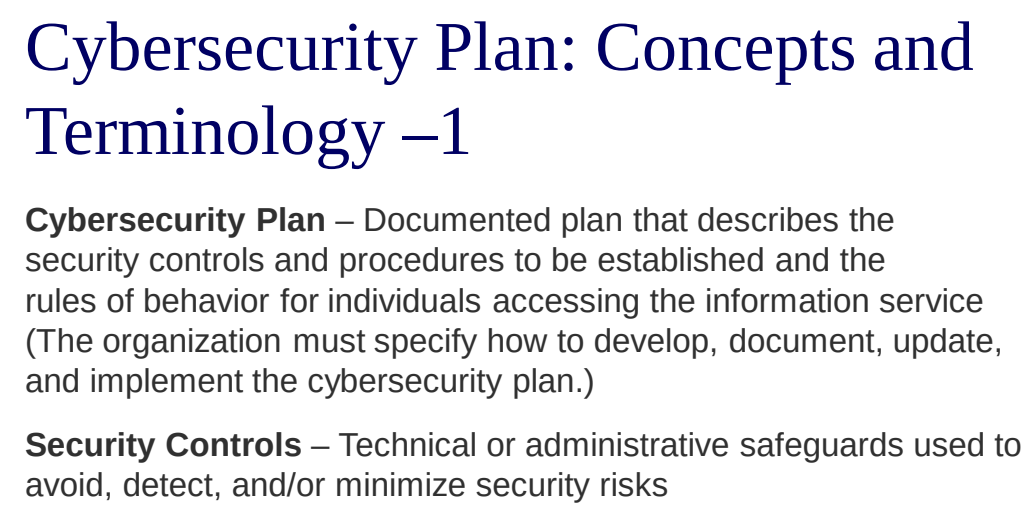
Cybersecurity Plan: Overview



**045 Instructor: Okay, so moving on to the next subdomain. So,

cybersecurity plan. The goal is to assess whether the organization has a defined and documented plan, and if the organization has a defined security policy in place. That's the aim of this section.

Cybersecurity Plan: Concepts and Terminology –1



**046 Terminology. Cybersecurity plan: Documented plan that describes the controls and procedures to be established and rules of behavior for individuals assessing the information service. Security controls-- I think we know what those are.

Cybersecurity Plan: Concepts and Terminology – 2

Cybersecurity Policy – An organization's formal governance that identifies any specific rules and regulations used to protect cyber assets

Example
All users must adhere to strict password complexity requirements.

Best Practice
Develop a cybersecurity plan that addresses all potential cyber aspects and is reviewed and updated regularly. Key personnel should know the plan, its contents, and their role.

**047 Cybersecurity policy. There's an example there of a very high-level policy: All users might adhere to strict password complexity requirements.

So a best practice in this area: Develop a cybersecurity plan that can address all potential cyber aspects and is reviewed and updated regularly. Key personnel should know the plan, its contents and their role in the plan.

Cybersecurity Plan: Training Tips

Possible Inconsistency – Question 15.2 (Cybersecurity Forces) cannot be answered "Yes" if Question 10.2 (Cybersecurity Plan) is answered "No."

Question 10.2 Is there a cybersecurity plan covering this CCS?	☑ No ❑ Yes

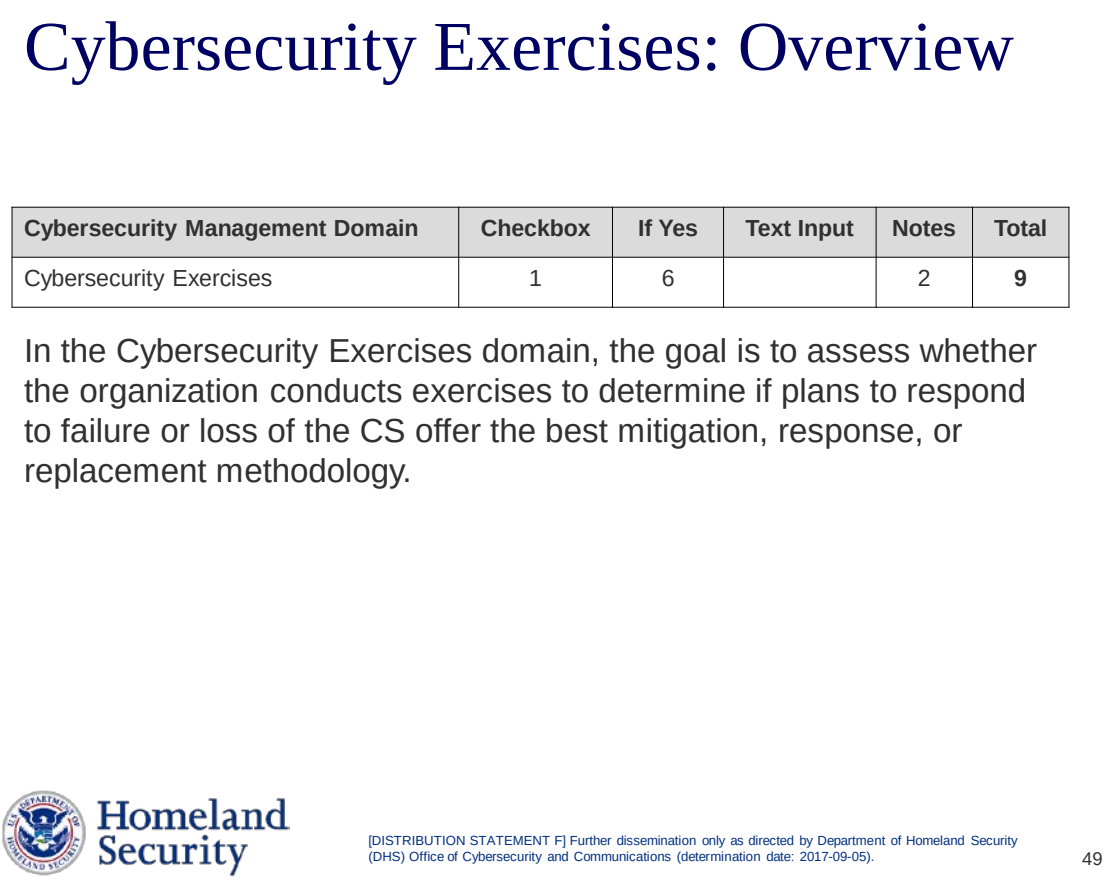
**048 Training tips in this area. Question 15.2 cannot be answered yes if Question 10.2 is answered no. Question 10.2: Is there a cybersecurity plan covering the CCS? So Question 15.2, which I don't have on a slide--

Student: "Are cybersecurity personnel trained on said security plan?"

Instructor: Right. So it becomes pretty obvious how you can end up in that inconsistency. So the idea of this is to make you guys aware of it so when you get all the way to Section 15, you kind of recall, "Hey,

they're saying yes here, but I don't think they had a plan."

Cybersecurity Exercises: Overview



**049 Moving on cybersecurity exercise. The goal here is to assess whether the organization conducts exercises to determine if plans to respond to a failure or loss of the service offers the best mitigation, response or replacement methodology.

Cybersecurity Exercises: Concepts and Terminology

Tabletop – A type of practical or simulated exercise typically talked about but not executed (This exercise usually involves senior-level staff members.)

Functional – A type of specialized operational exercise that involves some hands-on action by cybersecurity staff to respond to scenarios

Full Scale – A simulated or actual event that typically requires the entire organization to practice

Best Practice

Conduct cybersecurity exercises for reasons beyond simple regulatory compliance. Document and review the results.

Homeland Security

50

**050 Terminology in this section. Tabletop, functional, full scale. There's differences between them.

Best practice: Conduct cybersecurity exercises for reasons beyond simple regulatory compliance. Document and review the results. That exercise is going to be the only real time they know if what they plan will work, unless they've faced an actual incident. There wasn't one time in my experience of developing plans that I didn't learn something during an exercise of like, "Wow, that would not have worked." There's always something you're going to learn. It's never perfect out of the gate.

Cybersecurity Exercises: Training Tips

Review All Options – Some of the options available in Question 11.1, Subpart 1 (Cybersecurity Management) (e.g., cyber awareness and training) that may be performed in support of enterprise operations would still benefit the CS. Thus, they are still in scope, and the participant should select "Yes" to Question 11.1.

Question 11.1 Does the organization conduct cybersecurity exercises specific to the CCS?	❑ No ☑ Yes

Question 11.1, Subpart 1 For what purpose(s)? *(Check all that apply.)*	☑ Cyber awareness and training ❑ Service testing ❑ Continuity planning ❑ Disaster recovery

Homeland Security

51

**051 Tips in this area. Review all options. Some of the options available in Question 11.1 that may be performed in support of enterprise operations would still benefit the critical service. Thus, they are still in scope and the participant should select yes. So they may initially say no to, "Does the organization conduct cybersecurity exercises specific to the CCS?", but notice in 11.1, if you're doing cyber awareness training in certain other aspects, you may be doing it globally, but that also still affects the critical service. So you'd want to give them credit for that. That training does benefit the critical service. So as you're reviewing

these, you want to kind of take that look. Some of these options may not have been put in place specifically for the service but they still do benefit the service.

Information Sharing: Overview

Information Sharing: Overview

Cybersecurity Management Domain	Checkbox	If Yes	Text Input	Notes	Total
Information Sharing	6	13		4	**23**

In Information Sharing, the goal is to assess the organization's policy on

- processing, sharing, and receiving vulnerability and threat information and
- reporting cybersecurity incidents to outside organizations and communicating related information to internal personnel.

**052 Next subdomain: Information sharing. The goal is to assess the organization's policy on processing, sharing and receiving vulnerability and threat information. Also reporting cybersecurity incidents to outside organizations and communicating relevant information to internal personnel.

Information Sharing: Concepts and Terminology –1

Information Sharing – The process wherein private companies and government agencies participate in formal programs to exchange data on cybersecurity threats and vulnerabilities (Through these programs, organizations develop partnerships and share substantive information with each other to facilitate the defense of the CS.)

Threat Intelligence – Evidence-based knowledge, including context, mechanisms, indicators, implications, and actionable advice about an existing or emerging threat to information technology assets that can be used to inform decisions regarding the subject's response to that menace or hazard

**053 Terminology. Information sharing. Threat intelligence: Evidence-based knowledge including context, mechanisms, indicators, etcetera, actionable advice about an existing or an emerging threat-- some of the aspects of that.

Information Sharing: Concepts and Terminology –2

Vulnerability – A security flaw or weakness in software that can be exploited by a threat to compromise or cause damage to user data or degrade or deny the availability and performance of the CS

Automated Indicator Sharing (AIS) – The Department of Homeland Security's (DHS's) free Automated Indicator Sharing (AIS) capability that enables the exchange of cyber threat indicators between the Federal Government and the private sector at machine speed (Threat indicators are pieces of information like malicious IP addresses or the sender address of a phishing email, although they can also be much more complicated.)

**054 Vulnerability. Again, it's not a threat. This is a flaw or weakness that a threat could exploit. Automated indicator sharing-- I'm sure all you guys are familiar with that.

Information Sharing: Concepts and Terminology –3

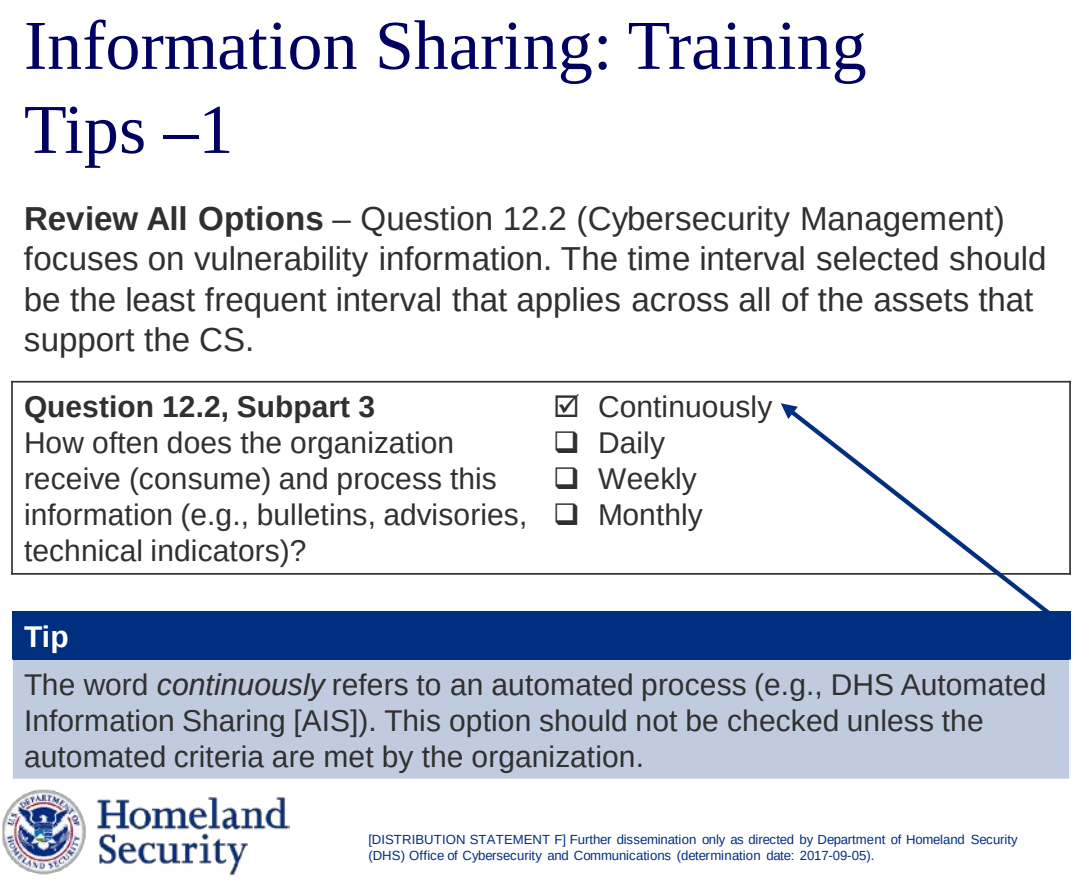
Indicator of Compromise (IOC) – A computer forensic artifact observed on a CS that, with high confidence, indicates an intrusion (Typical IOCs are virus signatures, IP addresses, MD5 hashes of malware files, and URL/domain names of botnet command and control servers.)

Best Practice

Gather cybersecurity threat and vulnerability information from external partners and analyze it. Share it with external partners and internal cybersecurity personnel.

**055 Indicators of compromise: A computer or forensics artifact observed on a critical service that with high confidence indicates an intrusion. Typical IOCs are virus signatures, IP addresses, MD5 hashes, malware, etcetera.

A best practice in this area: Gather cybersecurity threat and vulnerability information from external partners and analyze it. Share it with external partners and internal cybersecurity personnel.

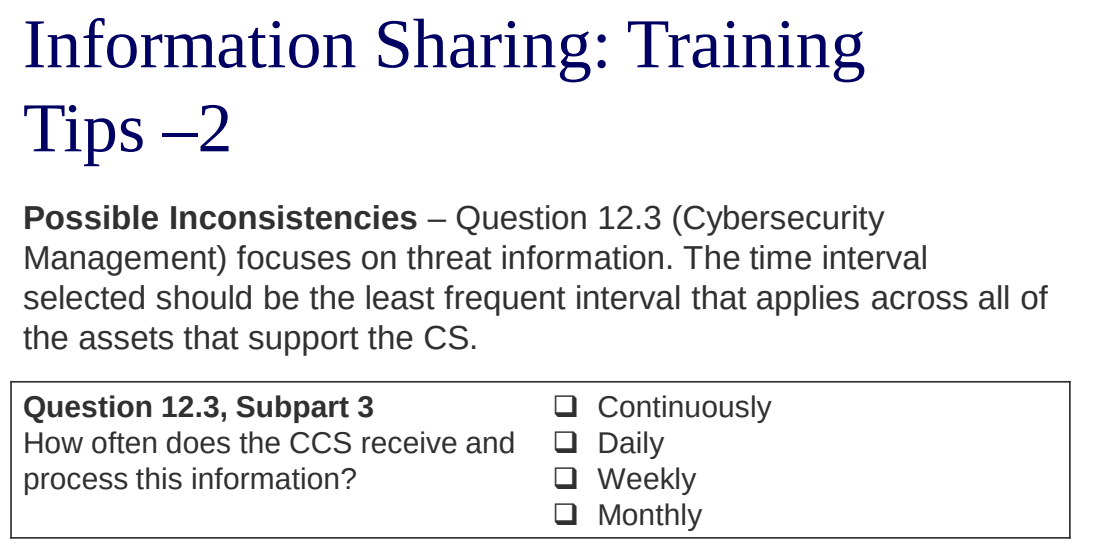


**056 What are the tips in this area? Again, another "Review all options." Question 12.2: Focus on vulnerability information. The time interval selected should be the least frequent interval that applies across all assets that support the critical service. So if you think about that discussion this morning with the least common denominator, that's what we're saying here, right? The least effective implementation.

Now, the tip here is the word "continuously"-- the additional tip here refers to an automated process. That's the intent of the CS. The question I had when I first saw this

is: If I have someone there that's looking at something every hour, is that considered continuous? And that's how we arrived at what we're really talking about in the CIS is that it should be kind of an automated process. Make sense? Am I losing you guys?

Information Sharing: Training Tips –2



**057 There's a lot here. That's why I'm kind of looking at everybody's faces. Training Tip 2: Possible inconsistency. Question 12.3 focuses on threat information. The time interval selected should be the least frequent interval that applies across all of the assets that support the CS.

Information Sharing: Training Tips –1

Review All Options – Question 12.2 (Cybersecurity Management) focuses on vulnerability information. The time interval selected should be the least frequent interval that applies across all of the assets that support the CS.

Question 12.2, Subpart 3	
How often does the organization receive (consume) and process this information (e.g., bulletins, advisories, technical indicators)?	☑ Continuously ❑ Daily ❑ Weekly ❑ Monthly

Tip

The word *continuously* refers to an automated process (e.g., DHS Automated Information Sharing [AIS]). This option should not be checked unless the automated criteria are met by the organization.

Homeland Security

56

**056 This is 12.2.

Information Sharing: Training Tips –2

Possible Inconsistencies – Question 12.3 (Cybersecurity Management) focuses on threat information. The time interval selected should be the least frequent interval that applies across all of the assets that support the CS.

Question 12.3, Subpart 3 How often does the CCS receive and process this information?	❑ Continuously ❑ Daily ❑ Weekly ❑ Monthly

**057 This is 12.3. How often does the CCS receive and process information? So there's actually kind of two aspects to this. Not only should it be the least effective interval that it's done, but it's really kind of a compound question. It's "receive and process this information". So not just looking at the received component.

Information Sharing: Training Tips –3

Possible Inconsistencies – In Question 13.1, Subpart 4 (Cybersecurity Management) the "Phone communications" option implies that a structured process exists with established bridge lines, etc.

Question 13.1, Subpart 4 What methods are used to communicate? (*Check all that apply.*)	❑ Ad-hoc meetings ❑ Recurring meetings ❑ Email communications ❑ Web-based delivery – not email (e.g., internal site, social media) ❑ Phone communications ❑ Other

**058 Tip 3 in this area: If question 13.1 subpart 4-- in Question 13.1 subpart 4-- the phone communications option implies that a structured process exists with established phone bridge lines. So when it asks about phone communications here, it's really talking about phone communications in this area. So you would have established call trees, established lines, etcetera. It's very specific to that. So it's more of a clarification.

Cybersecurity Forces

Table of Contents

Cybersecurity Forces

Cyber Infrastructure Survey (CIS) Training Course

Homeland Security

**059 The next domain that we will look at before taking a break is cybersecurity forces.

Cybersecurity Forces Domain –1

This part of the survey assesses whether the organization has assigned personnel to its cybersecurity operations and how they are trained. Specifically, it assesses

- the roles and responsibilities of the positions within the organization that support the CS and
- whether personnel charged with day-to-day CS operations receive cybersecurity training.

**060 Cybersecurity forces domain. This part of the survey assesses whether the organization has assigned personnel to its cybersecurity operations and how they are trained. Specifically it assesses the roles and responsibilities of the positions and whether the personnel charged with day-to-day operations receives cybersecurity training. That's what it's trying to get at.

Cybersecurity Forces Domain –2

Cybersecurity Forces Domain	Checkbox	If Yes	Text Input	Notes	Total
Personnel	4	6		2	**12**
Cybersecurity Training	4	5		2	**11**
Total	**8**	**11**		**4**	**23**

This domain contains a total of **23** questions.

- There are 8 simple Checkbox responses.
- There are 11 If-Yes questions, which require an additional response if the parent question is answered “Yes.”
- There are 4 Notes questions.

Homeland Security

**061 Another view by the numbers. It's a much smaller area.

Personnel: Overview

Cybersecurity Forces Domain	Checkbox	If Yes	Text Input	Notes	Total
Personnel	4	6		2	**12**

In Personnel, the goal is to assess whether the organization

- has formally established positions with responsibilities for its cybersecurity and the CS and
- conducts background checks on cybersecurity personnel.

**062 The first one, personnel. The goal is to assess whether the organization has formally established positions with responsibilities and conduct background checks on security personnel.

Personnel: Concepts and Terminology –1

Security Architect – Personnel responsible for designing, building, and overseeing the implementation of network and computer security for an organization

CERT or Computer Security Incident Response Team (CSIRT) – A team that focuses on coordinating a response to a cyber incident (These teams provide alerts and incident handling guidelines.)

**063 Terminology important to this section: A security architect, a CERT or CCERT. We've talked about some of this earlier.

Personnel: Concepts and Terminology –2

Background Check – An investigation conducted to examine criminal, commercial, and financial records of an individual (potential hire or current employee) to identify potential safety or security risks

Best Practice

Establish a policy that holds personnel accountable for their position and duties and requires recurring background checks on all personnel to mitigate risks due to insider threats.

Homeland Security

64

**064 Background checks. I believe everybody here would be familiar with that.

A best practice in this area: Establish a policy that holds personnel accountable for their position and duties and requires recurring background checks on all personnel to mitigate risk to insider threat.

Personnel: Training Tips –1

Possible Inconsistency – If Question 3.2 (Cybersecurity Management) is answered "Yes" and the option "Operational/Functional" is checked as a specialized area, it is expected one or more cybersecurity positions will be checked in Question 14.1 (Cybersecurity Forces).

Question 3.2 Are there any other cybersecurity leaders with cyber responsibilities?	☑ Yes ❑ No If yes, where do they specialize? (Check all that apply.) ☑ Operational/functional ❑ Service ❑ Enterprise/governance ❑ Other _____

Homeland Security

65

**065 Training Tip 1: Possible inconsistency. So what you're going to start seeing now potentially is some of the corresponding ones. As you get later into the domains, some of these might be repeated just as a way of enforcing it. If Question 3.2 is answered yes, and the option "operational/functional" is checked as a specialized area, it is expected that one or more of the positions will be checked in Question 14.1.

Personnel: Training Tips –2

Possible Inconsistency - If Question 3.2 (Cybersecurity Management) is answered "Yes" and the specialized area "Operational/Functional" is selected, answering "None of the above" to Question 14.1 (Cybersecurity Forces) would be inconsistent.

Question 14.1 Are the following positions formalized? (*Check all that apply.*)	Within your organization, ❑ Cybersecurity Policy and Planning Coordinator ❑ Cybersecurity Training Official ❑ Cybersecurity Incident Response Team Lead/Incident Commander ❑ CERT Staff/Triage Staff ❑ None of the above Within the CCS environment, ❑ Cybersecurity Exercise Official ❑ Security OPS Personnel ❑ Cybersecurity Threat Coordinator ❑ IT Controls and Compliance Staff ❑ Security Architect ❑ Application Admin/System Admin. ❑ None of the above

Homeland Security

66

**066 That is showing you everything available in 14.1.

Personnel: Training Tips –3

Possible Inconsistency – The answers to Questions 3.3 and 3.4 (Cybersecurity Management) should be checked against the answer to Question 14.3 (Cybersecurity Forces) since it relates to background investigations/reviews for contractors and vendors.

Question 3.3 Is there a third-party contract arrangement for primary cybersecurity management for the CCS?	❑ No ❑ Yes

Question 3.4 Are cybersecurity contractors or vendors used for day-to-day work? (Check all that apply.)	❑ Contractors ❑ Vendors ❑ N/A

Homeland Security

67

**067 So let's look at Training Tip 3. The answers to Question 3.3 and 3.4 should be checked against the answer to question 14.3. So you can see, we're further down in the assessment and now you got to think of it in a reverse order. Again, since it relates to background checks and reviews for contractors and vendors, so is there a third-party contract arrangement? If you answer yes, are cybersecurity contractors or vendors used for day-to-day work? Your selecting, say, both.

Personnel: Training Tips –4

Possible Inconsistency – The answer to Question 14.3 (Cybersecurity Forces) related to contractors and/or vendors should be consistent with the answers to Questions 3.3 and 3.4 (Cybersecurity Management). Answering "Yes" assumes that contractors and/or vendors have first been confirmed to be associated with the organization.

Question 14.3 Are background checks conducted for organizational and supporting personnel?	If applicable, contract cybersecurity personnel ❑ N/A ❑ No ❑ Yes If applicable, cybersecurity vendors ❑ N/A ❑ No ❑ Yes

Homeland Security

**068 If you look at it from this point of view you would not normally expect to see "Not applicable" here.

Cybersecurity Training: Overview

Cybersecurity Forces Domain	Checkbox	If Yes	Text Input	Notes	Total
Cybersecurity Training	4	5		2	**11**

In Cybersecurity Training, the goal is to assess the organization's training program, practices, and standards.

**069 So the second part, or the second subarea: Cybersecurity training. The goal is to assess the organization's training program and practices and standards.

Cybersecurity Training: Concepts and Terminology –1

International Standardization Organization (ISO) 27001 – International security management standard that specifies security management best practices and comprehensive security controls that can be used to reduce risks

Cybersecurity Plan – A documented strategic approach to securing an organization's cyber assets and approach to business continuity

Risk Management – The process of identifying, analyzing, and mitigating risks to organizational assets that could adversely affect the critical service

**070 So some of the things you'll see in this section is International Standard Organization is one of the potential standards that's mentioned, cybersecurity plan, risk management. I believe we're all familiar with that.

Cybersecurity Training: Concepts and Terminology –2

Incident Response – Processes and procedures that an organization uses to identify, investigate, and respond to potential security-related incidents

Threat Analysis – The process of examining the sources of threat and evaluating them in relation to an information system's vulnerabilities

Best Practice

Perform, evaluate, and update training regularly.

Homeland Security

**071 Incident response. Threat analysis again. A best practice in this area would be to perform, evaluate, and update training regularly.

Cybersecurity Training: Training Tips –1

Clarification – Question 15.1 (Cybersecurity Training) assesses the technical training of personnel (e.g., network admins, server admins, incident response) involved specifically with cyber operations that support the CS.

Question 15.1	❑ No ☑ Yes
Do cybersecurity personnel involved in day-to-day CCS operations receive cybersecurity training?	

Tip

Do not consider the training of CS users when responding to this question.

72

**072 So let's look at this Training Tip 1. Question 15.1 addresses the technical training of personnel involved specifically with cyber operations that support the critical service. So this is geared more to the network administrators, the server administrators, incident response personnel.

Instructor: So this is technical training for them. This isn't general awareness training. That's where this question is aimed. Do cybersecurity personnel involved in day-to-day critical service operations receive cybersecurity training? So it's more of that technical nature.

Do not consider the training of CS users when responding to this question. This is specifically about people involved in the day-to-day operations of the critical service.

Cybersecurity Training Training Tips –2

Cybersecurity Training Training Tips –2

Possible Inconsistency – If Question 15.2 (Cybersecurity Training) is answered "Yes," check that Question 10.2 (Cybersecurity Management) is also answered "Yes."

Question 10.2 Is there a Cybersecurity Plan covering this CSS?	❑ No ☑ Yes

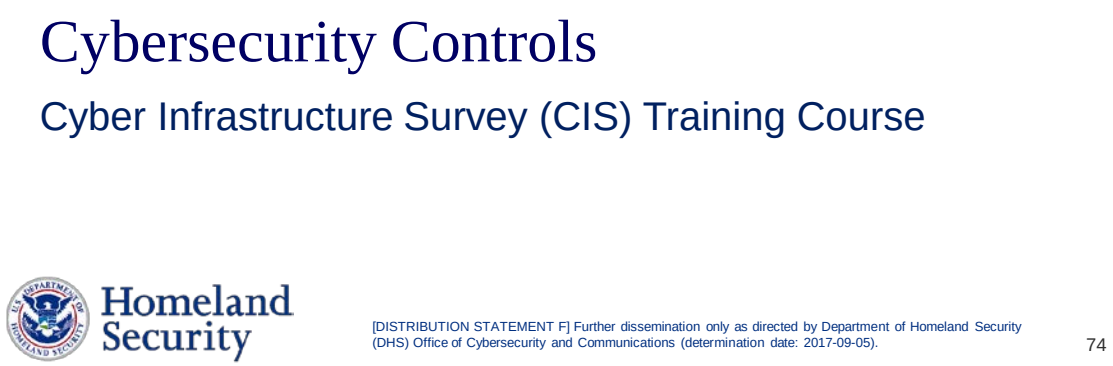
Question 15.2 Are cybersecurity personnel trained on the cybersecurity plan?	❑ No ☑ Yes

Homeland Security

**073 Tip 2: If Question 15.2 is answered yes, check that Question 10.2 is also answered yes. This is the reverse of what we saw earlier, I believe. Or no, it's not, actually. Is there a cybersecurity plan? Yes. Are cybersecurity personnel trained on that plan? They shouldn't be answering yes to one and no to the other.

Cybersecurity Controls

Table of Contents



**074 Instructor: All right. We're going to take a deep dive into Cybersecurity Controls domain.

Cybersecurity Controls Domain –1

This part of the survey assesses the security controls that the organization has implemented to protect the CS. Specifically, it assesses the

- types of controls deployed to protect the CS,
- measures used to control privileges,
- implementation of security controls to limit access, and
- security measures in place to prevent inadvertent access to sensitive data.

**075 So at this part of the survey we're going to assess the types of controls deployed to protect the critical service, measures used to control privileges, implementation of security controls, the limit access and also security measures in place.

Cybersecurity Controls Domain –2

Cybersecurity Controls Domain	Checkbox	If Yes	Text Input	Notes	Total
Authentication and Authorization Controls	9	7		2	**18**
Access Controls	5	3		4	**12**
Cybersecurity Measures	6	37		6	**49**
Information Protection	2	4		2	**8**
User Training	1	3		2	**6**
Defense Sophistication and Compensating Controls	1	1			**2**
Total	**24**	**55**		**16**	**95**

This domain contains a total of **95** questions.

- There are 24 simple Checkbox responses.
- There are 55 If-Yes questions.
- There are 16 Notes questions.

Homeland Security

76

**076 Here's a breakdown of the domain. Second largest domain. You can see there's six subdomains to it.

Authentication and Authorization Controls: Overview

Cybersecurity Controls Domain	Checkbox	If Yes	Text Input	Notes	Total
Authentication and Authorization Controls	9	7		2	**18**

In Authentication and Authorization, the goal is to

- identify the basis for the authentication and authorization controls in place to limit access to the CS and
- assess the common authentication and authorization practices and techniques used in the CS.

**077 So the first subdomain is going to be Authentication and Authorization. We're going to attempt to identify the basis for authentication and authorization controls and assess common authentication and authorization practices.

Authentication and Authorization Controls: Concepts and Terminology –1

Authorization – Access privileges granted to a user, program, or process or the act of granting those privileges

Multi-Factor Authentication – A method of authentication that requires the user to use two or more factors from the following list:

- something you know (e.g., password/PIN),
- something you have (e.g., cryptographic identification device or token), or
- something you are (e.g., biometric signature).

Identity Proofing – The process of collecting and verifying information about a person to issue credentials to them

Homeland Security

**078 So some concepts and terminology. I think most of us know authorization, multi-factor authentication, identity proofing are going to be some of the concepts that come up in this, this section.

Authentication and Authorization Controls: Concepts and Terminology –2

Principle of Least Privilege – The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function

Best Practice

Provide access to the CS to only authorized personnel. Establish access controls that limit access only to legitimate users and incorporate the principle of least privilege to guide their access to systems and data.

Homeland Security

79

**079 Principle of least privilege. Principle that a security architect should be designed, architecture should be designed, so that each entity is granted the minimum security resources and authorizations that the entity needs to perform its functions.

Best practice. Provide access to the critical service to only authorize personnel, establish access controls that limit access only to legitimate users and incorporate the principle of least privilege.

Authorization and Authentication Controls: Training Tips –1

Clarification – In Question 16.2 (Cybersecurity Controls), the phrase "All user accounts" refers to a human user account and not a system service account.

Question 16.2 Which of the following measures does the organization employ to control authorization?	❑ All user accounts have an expiration date.

Homeland Security

**080 Authorization and authentication controls, the training tips. So in Question 16.2, Cybersecurity Controls, the phrase "All user accounts" refers to a human user account and not a system service account. So whenever you're answering this question, all user accounts have an expiration date, it means just that. Don't take into account any type of system service account that doesn't have an expiration assigned to it.

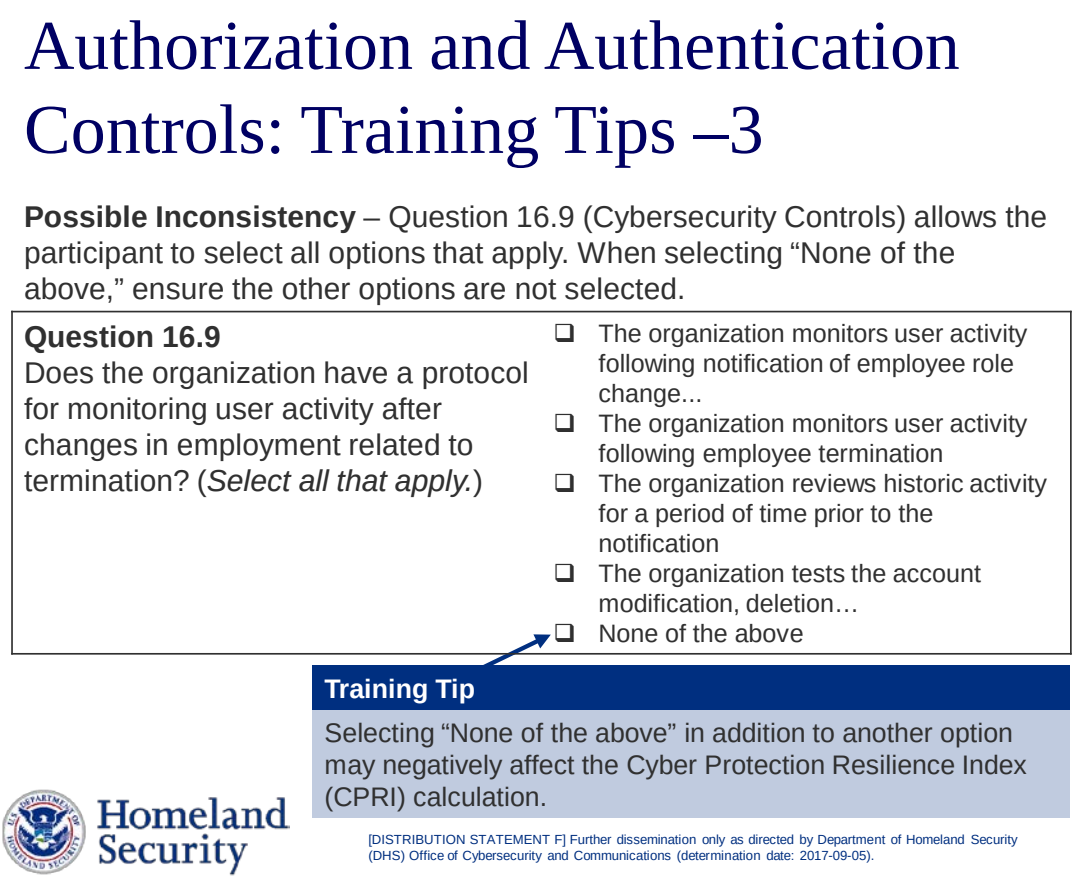
Authorization and Authentication Controls: Training Tips –2

Clarification – The response to Question 16.5 (Cybersecurity Controls) contains an error. “Organization disallows shared passwords…” should read “Organization disallows shared accounts…”

Question 16.5 Which of the following password management policies are implemented for the CCS?	❑ Organization disallows shared passwords forcing each account holder and service to have its own username/password.

Homeland Security

**081 Training tip number two for this section. The response to Question 16.5 contains an error. "Organizations disallows shared passwords..." should read, "Organizations disallows shared accounts..." So you can see in the one response here, this is exactly what it says. Organization disallows shared passwords forcing each account holder and service to have its own username and password. That should be shared accounts.



**082 Training tip number three. Question 16.9 allows the participant to select all options that apply. When selecting "None of the above," ensure the other options are not selected.

So selecting this too is going to affect the CPRI score negatively, so it's just a QA thing to keep in mind, something they're looking out for. Any questions?

Access Controls: Overview

Cybersecurity Controls Domain	Checkbox	If Yes	Text Input	Notes	Total
Access Controls	5	3		4	**12**

In Access Controls, the goal is to assess the organization's implementation of security controls to

- limit access across the boundaries and
- prevent exploitation of the access path.

**083 All right. Access Controls. So we're going to look at security controls that limit access across boundaries and prevent exploitation of access paths.

Access Controls: Concepts and Terminology –1

Remote Access – Access to an organization's information system by a user (or an information system acting on behalf of a user) communicating through an external network outside of the organization's security perimeter

Encryption – Conversion of plaintext to ciphertext through the use of a cryptographic algorithm

Firewall – A gateway that limits access between networks in accordance with local security policies

**084 Some terminology you need to be familiar with. Remote access, encryption, firewall.

Instructor: Intrusion Detection Systems. Web proxy. An application that breaks the connection between client and server. This method effectively closes straight path between internal and external networks, making it more difficult for an attacker to obtain internal access.

Access Controls: Concepts and Terminology –3

White List – A list of programs, domains, or IP addresses that are explicitly allowed to run because they are known and trusted

Black List – A list of programs, domains, or IP addresses that are explicitly not allowed to run because they may be associated with malicious activity or cyber threats

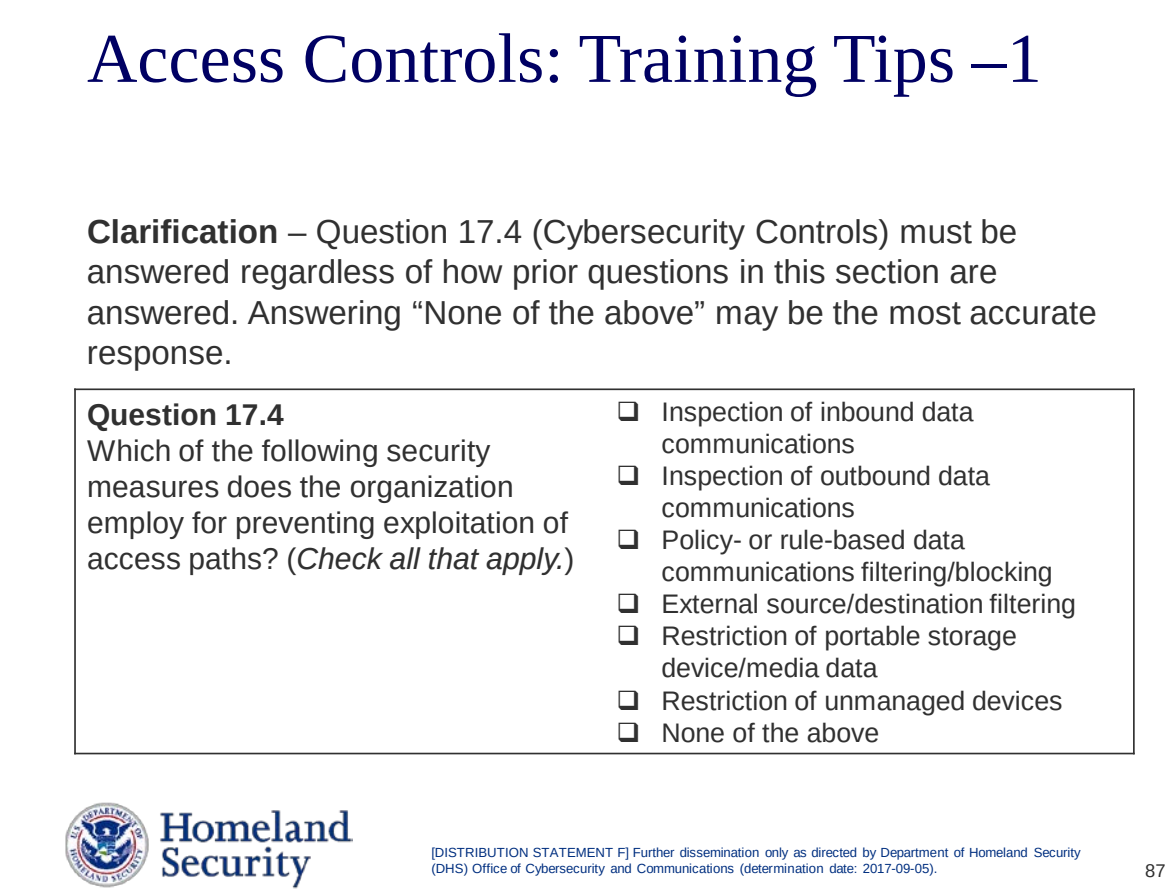
Best Practices

Establish control objectives and implement security controls that restrict incoming and outgoing connections.

Document control objectives and controls for reference and analysis.

**086 White List. Black List. White listing, only allowing certain programs to run on applications. Black List, disallowing specific things from running on the system.

So best practice. Establish control objectives and implement security controls that restrict incoming and outgoing connections, document control objectives and controls for reference and analysis.

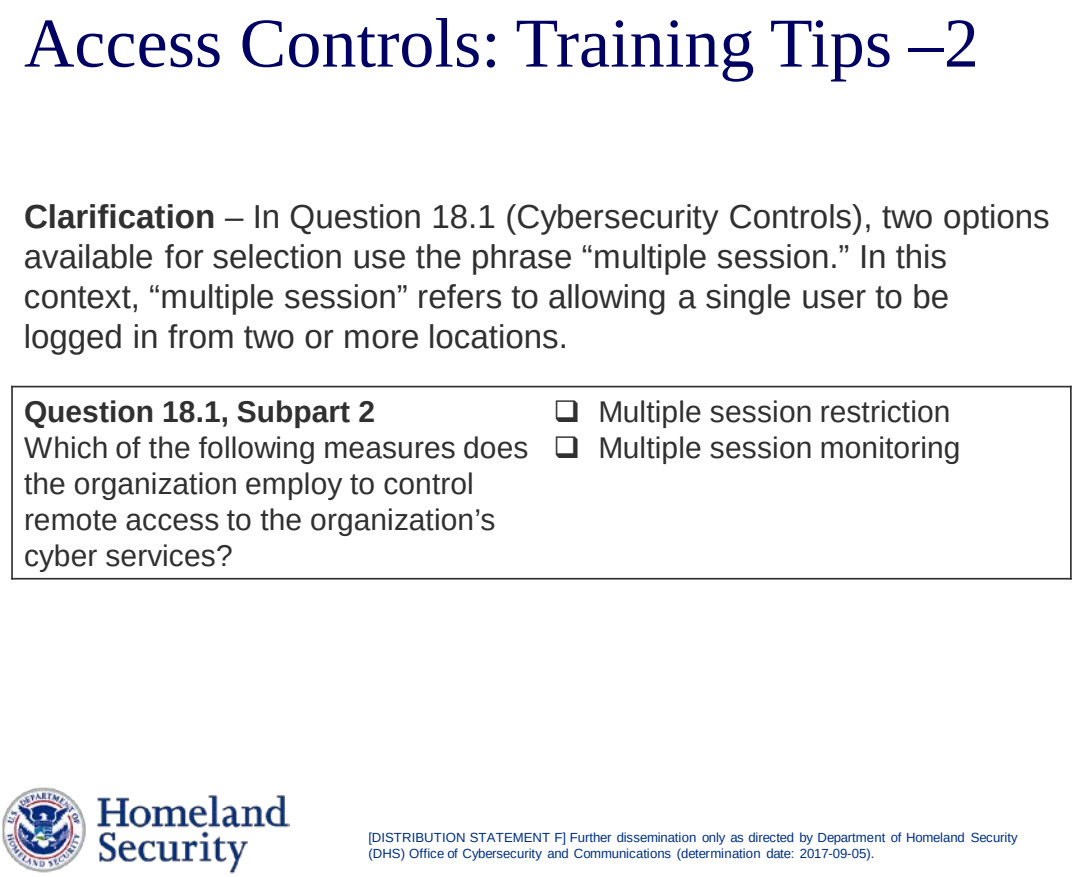


**087 Instructor: All right. Training tip number one for access controls. Questions 17.4. Question 17.4 must be answered regardless of how prior questions in this section are answered. Answering "None of the above" may be the most accurate response.

So the question is, "Which of the following security measures does the organization employ for preventing exploitation of access paths?" A valid answer is "None of the above," but make sure you answer this regardless of what comes beforehand. I don't have a companion guide.

Instructor: Yeah. So if you look on Page 20, you're going to see that there's 17.1, 2 and 3, right? Regardless of how those are answered, you still want to answer 17.4. Right. And in this case, "None of the above" is a valid answer because they're specifically looking for these options here. You may not have any of them.

Access Controls: Training Tips –2



**088 Training Tip Number 2. In Question 18.1, two options available for selection use the phrase "multiple session." In this context, "multiple session" refers to allowing a single user to be logged in from two or

more locations. So just a clarification from there on what they're looking for with multiple sessions. Good?

Cybersecurity Measures: Overview

Cybersecurity Measures: Overview

Cybersecurity Controls Domain	Checkbox	If Yes	Text Input	Notes	Total
Cybersecurity Measures	6	37		6	**49**

In Cybersecurity Measures, the goal is to assess how the organization uses

- countermeasures to detect malicious code and
- cybersecurity measures to monitor the network.

**089 Okay. Cybersecurity Measures. We're going to look at how an organization deploys countermeasures to detect malicious code as well as the measures that are in place to monitor the network.

Cybersecurity Measures: Concepts and Terminology –1

Heuristic-Based Virus Detection – A method used by an antivirus program designed to detect previously unknown or unobserved malicious activity based on rules and/or algorithms

Signature-Based Virus Detection – A method that detects malicious activity by looking for specific patterns, such as a byte sequence in network traffic or a known malicious instruction sequence

Data-Loss Prevention – A strategy that ensures sensitive or critical information is not allowed to be sent outside the organization's network security perimeter without authorization

**090 Some key concepts. Heuristic-based virus detection. So a method used by an antivirus program designed to detect previously unknown or unobserved malicious activity based on certain rules and/or algorithms.

It's different from signature-based, which is it detects malicious code looking for specific patterns and known malicious instruction sequences.

Also talks about and brings the concept of data-loss prevention in this section.

Cybersecurity Measures: Concepts and Terminology –2

Malicious Code – Code that is intended to cause undesired effects, security breaches, or damage to a system

Best Practice
Regularly monitor and scan networks for unauthorized access/activities. Conduct this scanning using near-real-time, automated, or manual techniques in any combination based on the organization's risk tolerance.

Homeland Security

**091 Malicious code. The best practice. Regularly monitor and scan networks for authorized access/activities. Conduct the scanning using near-real-time, automated or manual techniques in any combination based on the organization's risk tolerance.

Cybersecurity Measures: Training Tips

Clarification – When cybersecurity measures are implemented on the network to monitor assets and detect cybersecurity events, give full credit, even if the sensors are not focused specifically on the CS. Deployed devices that protect the organization's overall security perimeter also support the CS.

Question 20.1
Which of the following cybersecurity measures does the organization employ for monitoring of assets and networks related to CCS?

- ❑ Automated security event response
- ❑ Automated security event Alerting
- ❑ Near-real-time monitoring for malicious code
- ❑ Near-real-time monitoring for unauthorized access
- ❑ Near-real-time monitoring for unauthorized software
- ❑ Near-real-time network boundary intrusion detection
- ❑ Near-real-time network boundary traffic monitoring
- ❑ Near-real-time host intrusion monitoring
- ❑ Manual, non-real-time network monitoring based on audit logs
- ❑ None of the above

Homeland Security

92

**092 So training tip. When cybersecurity measures are implemented on the network to monitor assets and detect cybersecurity events, give full credit, even if the sensors are not focused specifically on the critical service. Deployed devices that protect the organization's overall security perimeter also support the critical service.

So this is a instance where they're instructing you to give credit because they have sensors in other places in the organizations that can prevent any type of attack or software getting through to the critical service, so give

credit where due whenever that's the case. So even though it's not deployed specifically for the critical service, they may say, "We have this," and use your best judgment to say, "Okay. Well, at some point that is going to give protection to the critical service."

Information Protection: Overview

Information Protection: Overview

Cybersecurity Controls Domain	Checkbox	If Yes	Text Input	Notes	Total
Information Protection	2	4		2	**8**

In Information Protection, the goal is to assess

- how the organization identifies and protects sensitive information and
- whether the organization properly manages sensitive information.

**093 Instructor: Information Protection. So we're going to assess how the organization identifies and protects sensitive information and whether the organization properly manages sensitive information.

Information Protection: Concepts and Terminology –1

Personally Identifiable Information – Data that could be used to identify a specific individual or is directly linked to a certain individual

Data at Rest – Information located on storage devices that are components of information systems

Data in Transit/Motion – Data that is being transmitted over internal or external networks between all types of information system components

**094 Some concepts and terminology in this section are going to be personally identifiable information, data at rest, data in transit, data in motion. Think everyone's familiar with these terms.

Information Protection: Concepts and Terminology –2

Data Replication – Copying and moving data between an organization's servers or sites/locations

Data Backup – Making a copy or copies of data

Best Practice
Identify, categorize, and appropriately secure information assets. Back up all sensitive information assets and validate the backup.

Homeland Security

**095 Data replication. Copying and moving data between an organization's servers. Data backup.

So best practice. Identify, categorize and appropriate secure information assets. Back up all sensitive information assets and validate the backup.

User Training: Overview

Cybersecurity Controls Domain	Checkbox	If Yes	Text Input	Notes	Total
User Training	1	3		2	**6**

In User Training, the goal is to assess when CS users are given

- cybersecurity training and
- access to the network.

**096 There's no training tips for that section. So the next subdomain is going to be User Training. We're going to assess when critical servers are given cybersecurity training and when they're given access to the network in this section.

User Training: Concepts and Terminology

Acceptable Use Policy – A set of rules that restrict the ways the network, website, or system may be used and outlines how it should be used

Password Policy – A set of rules that establish a standard for creating strong passwords, protecting those passwords, and how often they should change

Best Practice

Train users before granting them network and/or system level access. Regularly review training effectiveness and provide additional/refresher training.

Homeland Security

97

**097 Concepts and Terminology. Acceptable use policy. A set of rules that restricts the way the network, website or system may be used and outlines how it should be used. Password policy.

Best practice. Train users before granting them network and/or system level access. Regularly review training effectiveness and provide additional refresher training.

User Training: Training Tips

Clarification – Question 23.1 (Cybersecurity Controls) and its subparts pertain to the CS end-user training.

Question 23.1 Does the organization provide training on cybersecurity for CCS users/operators on a regular basis?	❑ No ❑ Yes

**098 So training tip. Question 23.1 and its subparts pertain to the critical service end-user training. So does the organization provide training on cybersecurity for the critical service users operators on a regular basis? Earlier distinction was the training was specific for cybersecurity personnel focuses on more technical cybersecurity training. This section truly is for end-user training of the critical service.

Student: So would overall organizational cybersecurity training qualify for this?

Instructor: I would say, "Yes," if it affects the end users of the critical service. Right? So if you look at Page 23 also, you'll see the complete list of options underneath that.

Instructor: Yeah. Yeah. So it's a similar concept to the cybersecurity measures if they're deploying it somewhere else and it stands to benefit the critical service.

Any other questions for this?

Instructor: So if I could, as you look at that, it's getting to the certain things that Gavin brought up earlier. You know, for example, one part of it is when does the organization provide this training, right? Before the user obtains access? Within a week? Thirty days? Right. So it's looking at different aspects of the training that they get, right?

Instructor: Yeah. And I was going to say, so the best practice is ideally you want to provide the training before you give access, but there are some options to capture. You know, they get this X-amount of time after they've already been given access to try and establish. But even though they have access, at least you're giving it to them at some point in time, but obviously quicker the better for that.

Defense Sophistication and Compensating Controls: Overview

Cybersecurity Controls Domain	Checkbox	If Yes	Text Input	Notes	Total
Defense Sophistication and Compensating Controls	1	1			**2**

In Defense Sophistication and Compensating Controls, the goal is to assess the sophistication of the defensive and compensating controls the organization uses.

**099 All right. Defense Sophistication and Compensating Controls. The goal is to assess the sophistication of the defensive and compensating controls the organization uses.

Defense Sophistication and Compensating Controls: Concepts and Terminology –1

Moving Target Defense (MTD) – Changing the computing environment in a controlled manner to increase attacker uncertainty and attack complexity and decrease the time available to the attacker to implement an attack

Network-Level MTD – MTD technique that includes changing the network topology (e.g., IP-hopping, using random port numbers, and configuring fake listening hosts)

Host-Level MTD – MTD technique that includes changing the host and OS-level resources, naming, and configuration

**100 So some key concepts and terminology that are defined in the CIS. So Moving Target Defense. Changing the computing environment in a controlled manner to increase attacker uncertainty and attack complexity and decrease the time available to the attacker to implement an attack.

Network-level Moving Target Defense. Includes changing the network topology, such as IP-hopping, using random port numbers and configuring fake listening hosts.

Host-level Moving Target Defense. Changing the host and OS-level

resources, naming and configuration are some examples of some sophisticated and compensating controls.

Defense Sophistication and Compensating Controls: Concepts and Terminology –2

**101 Student: How often do you see that?

Student: Zero.

Student: I haven't seen any yet, but I just wondered, how often have you- I've never answered that, "Yes" yet.

Instructor: It's not something I've seen often either.

Student: Okay.

Instructor: Right. There are some companies that do do it. Like Netflix is a good example with their chaosmonkey, right? They--

Student: chaosmonkey?

Instructor: Mm-hm. So it's an application they have that actively kills servers and so forth and processes and then--and they do this live, and the other one should pick up the slack.

Student: Mm.

Instructor: And they do this throughout their environment, right, to make sure that they can continue operations, for example. I don't--I've read about things like that, but I've not run across, on a personal level, how many--

Student: Oh, thank you. I just wondered--

Instructor: Mm-hm.

Student: --why that one was specifically called out. That was my thing.

Student: I've only seen it with defense contractors.

Student: Yeah.

Student: And with really large organizations. It's not usually financial organizations.

Student: Somebody that has, like, rotating data centers where they'll have--and their data centers are actually structured so that the operating systems in each data center's different so as they do a sunset rule, as the data center moves, you're moving from Windows platform to Linux platform to a hybrid platform just so that the bad guys never know what they're, you know, what you're using and stuff like that.

Instructor: Yep.

Student: They constantly keep scanning in order to keep up with it. So I've seen some of those advanced tactics, but not on anybody that we're probably going to target--

Student: Yeah.

Student: --these assessments for.

Instructor: Yeah. I believe the, you know, the purpose of the question is one, to find out if anyone is really doing anything, and to kind of be able to record those things and learn a little bit about them so that DHS can potentially then take that information and inform others, right?

Student: Thanks.

Instructor: And so best practice. Implement additional layers of compensating defenses to secure the critical service.

Defense Sophistication and Compensating Control: Training Tips

Clarification – In Question 24.1 (Cybersecurity Controls), “Advanced tactics and strategies…” means an innovative industry/sector leading practice and not just a good or best practice.

Question 24.1
Does your organization employ additional advanced tactics, strategies and/or specific layered defenses to compensate for a loss of primary controls specific to CCS? (Examples may include platform diversity, moving target defense, etc.)

Homeland Security

102

**102 Clarification training tip for this. In Question 24.1, "Advanced tactics and strategies..." means an innovative industry/sector leading practice, not just a good or best practice. So similar to conversation we just had.

Incident Response

Table of Contents

Incident Response

Cyber Infrastructure Survey (CIS) Training Course

103

**103 All right. Incident response.

Incident Response Domain –1

This domain identifies the organization's incident response and business continuity capability. Specifically, it assesses the organization's

- readiness to respond to a cybersecurity incident and
- ability to recover its CS from an incident with its cybersecurity controls in place.

**104 So this domain we're specifically going to look to assess the organization's readiness to respond to cybersecurity incidents and its ability to recover the critical service from an incident with its cybersecurity controls in place.

Incident Response Domain –2

Incident Response Domain	Checkbox	If Yes	Text Input	Notes	Total
Incident Response Measures	2	5		2	**9**
Alternate Site and Disaster Recovery	7	2	1	2	**12**
Total	**9**	**7**	**1**	**4**	**21**

This domain contains a total of **21** questions.

- There are 9 simple Checkbox responses.
- There are 7 If-Yes questions, which require an additional response if the parent question is answered “Yes.”
- There is 1 Text Input question.
- There are 4 Notes questions.

Homeland Security

105

**105 Question breakdown.

Incident Response Measures: Overview

Incident Response Domain	Checkbox	If Yes	Text Input	Notes	Total
Incident Response Measures	2	5		2	**9**

In Incident Response, the goal is to assess whether

- the organization has a fully documented incident response plan and
- personnel understand the policies and procedures outlined in the incident response plan.

106

**106 Two sections. So first one is going to be Incident Response Measures. Assess whether the organization has fully documented incident response plan and then also the see if personnel understand the policies and procedures outlined in the incident response plan.

Incident Response Measures: Concepts and Terminology –1

Incident Response – An organized approach to addressing and managing the aftermath of a security breach or attack (Incident Response consists of the following core phases: preparation, identification, containment, eradication, and recovery.)

Incident Handling – The actual steps or procedures taken to respond to violations of security policies and recommended practices

Data Breach – An incident in which sensitive, protected, or confidential data, such as intellectual property or records containing an employee or customer's name, has potentially been viewed, stolen, or used by an unauthorized individual

107

**107 Key concepts and terminology for this is going to be incident response. An organized approach to addressing and managing the aftermath of a security breach or attack. Incident handling. The actual steps or procedures taken to respond to the violation. Data breach.

Incident Response Measures: Concepts and Terminology –2

Priority Plan – A list that indicates the order in which facilities or facility types will be restored (For example, most utility providers prioritize and restore service to human health facilities—such as hospitals, water treatment service assets, and nursing homes—before other customers.)

Best Practice

Institute a plan that outlines how to respond to cyber incidents. Use the results from regular tests of the plan and the results from responses to actual incidents to make adjustments to the plan.

Homeland Security

108

**108 Priority plan. A list that indicates the order in which facilities or facility types will be restored.

So best practice. Institute a plan that outlines how to respond to cyber incidents. Use the results from regular tests of the plan and the results from responses to actual incidents to make adjustments to the plan.

Incident Response Measures: Training Tips –1

Possible Inconsistency – Question 25.1 (Incident Response) is an "If-Yes" question with five subparts. When answering Subpart 3, the answer "No incident response procedure exists" should be interpreted as "None of the above." The participant can select this answer even if Question 25.1 was answered "Yes."

Question 25.1 Does the organization have predefined plans for responding to cybersecurity incidents specific to the CCS?	❑ Planned procedures for network containment ❑ Planned procedures for malware containment(s) and boxing ❑ Planned procedures to rate limit in response to a distributed denial of service attack ❑ Planned procedures to respond to an unauthorized access to operationally sensitive information ❑ No incident response procedure exists
Question 25.1, Subpart 3 The organization has defined incident response procedures for handling cyber incidents specific to the CCS, which (at a minimum) contain: (*Check all that apply.*)	

Homeland Security

109

**109 Training Tip 1. Question 25.1 is an "If-Yes" question with five subparts. When answering Subpart 3, the answer "No incident response procedure exists" should be interpreted as, "None of the above." The participant can select this answer even if 25.1 was answered "Yes."

So "No incident response procedures exist" is the same as "None of the above." Good?

Incident Response Measures: Training Tips –2

Clarification – Question 25.1, Subpart 5 (Incident Response) should be answered according to the frequency defined in the documented policy/procedure for post-incident review. This guideline applies even if an incident has not occurred. A review is not something to be performed on an ad-hoc basis.

Question 25.1, Subpart 5 How often do you review responses to actual cyber incidents to see if they are consistent with the incident response procedures/plan specific to the CCS?	❑ Within a formally defined time after incident resolution, as part of follow-on actions ❑ Monthly ❑ Semiannually ❑ Annually ❑ Never

Homeland Security

110

**110 Training Tip 2. Question 25.1, Subpart 5 should be answered according to the frequency defined in the documented policy/procedure for post-incident review. This guideline applies even if an incident hasn't occurred. A review is not something to be formed on an ad-hoc basis.

So a lot of the times in the assessments I've been a part of, they'll say, "We haven't had to do this yet," but we kind of ask them, "Well, is there a frequency defined in your plan?" So really what we're looking for here is that they have a frequency for review documented in their plan somewhere. They may

have not exercised that yet or done the review because they haven't had an incident, but we're looking for a documented frequency.

Student: Frequency.

Instructor: Frequency. Yeah. Not just, "Well, if we had an incident, we'd do a review." A lot of times you'll hear, "Well, yeah. Of course if we had one, we'd do a review." We're looking for some evidence that it's procedurally done.

Alternate Site and Disaster Recovery

Alternate Site and Disaster Recovery

Incident Response Domain	Checkbox	If Yes	Text Input	Notes	Total
Alternate Site and Disaster Recovery	7	2	1	2	**12**

In Alternate Site and Disaster Recovery, the goal is to assess the

- organization's contingency procedures/capabilities and access to an alternate site,
- length of time required for the organization to recover the CS after a disaster, and
- whether the organization tests alternate site procedures.

**111 Instructor: Alternate Site and Disaster Recovery. So the goal

is to assess the organization's contingency procedures, capabilities and access to an alternate site. Length of time required for the organization to recover the critical service after a disaster, and whether the organization tests alternate site procedures.

Alternate Site and Disaster Recovery: Concepts and Terminology –1

Alternate Site and Disaster Recovery: Concepts and Terminology –1

Business Continuity – The capability of the organization to continue the delivery of products or services at acceptable, predefined levels following a disruptive incident

Severely Impacted – A CS that is running at a level considered "significantly lower output to no output" of work

Hot Site – A fully operational offsite data-processing facility equipped with hardware and software, that is used in the event of an information system disruption

**112 Some key concepts and terminology here is business continuity. Severely impacted. A critical service that is running at a level considered "significantly lower output to no output" of work.

Hot site. Fully operational offsite data-processing facility equipped with hardware and software, that is used in the event of an information disruption.

Alternate Site and Disaster Recovery: Concepts and Terminology –2

Alternate Site and Disaster Recovery: Concepts and Terminology –2

Cold Site – A backup facility that has the necessary electrical and physical components of a computer facility but does not have the computer equipment in place (The site is ready to receive the necessary replacement computer equipment in the event that the users must move from their main computing location to an alternate site.)

Warm Site – An environmentally conditioned workspace that is partially equipped with information systems and telecommunications equipment to support relocated operations in the event of a significant disruption

Best Practice

Establish a business contingency or continuity plan for recovery of the CS. The plan must describe the alternate location, technology and information requirements, restoration of data from backups, cybersecurity requirements, personnel, and operations, etc. to allow the CS to continue to perform.

Homeland Security

113

**113 We have cold site. Maybe a backup facility that has the necessary electrical and physical components but does not have the equipment in place. Can use that but you have to move some of your equipment over there.

Warm site. An environmentally conditioned workspace that is partially equipped with information systems and telecommunications

equipment. So the questions in this section are going to revolve around some of those concepts.

So best practice. Establish a business contingency or continuity plan for recovery of the critical service. The plan must describe the alternate location, the technology and information requirements, restoration of data from backup, cybersecurity requirements, personnel, etcetera, to allow the critical service to continue to perform.

Alternate Site and Disaster Recovery: Training Tips –1

Alternate Site and Disaster Recovery: Training Tips –1

Clarification – If Question 26.5 (Incident Response) is answered "Yes," going straight to Question 26.8 (Incident Response) may provide better flow and result in more accurate responses to Questions 26.6 and 26.7 (Incident Response).

Question 26.5 Does the organization employ measures to preserve cybersecurity of the CCS after a disruption or organization incident?	❑ No ☑ Yes

Question 26.8 Which of the following disaster measures does the organization have? (*Check all that apply.*)	❑ Alternate-site operations include… ❑ Recovery/reconstitution phases include… ❑ Organization has Continuity of CCS operations plans that include… ❑ Organization has CCS disaster recovery plans that include… ❑ Organization has business continuity plans that include… ❑ Organization has CCS backups of data… ❑ Organization has no documented measures.

Homeland Security

114

**114 Training Tip 1 for Alternate Site and Disaster Recovery. If

Question 26.5 is answered "Yes," going straight to Question 26.8 may provide better flow and result in more accurate responses to questions 26.5 and 26.7.

So if we answer 26.5 "Yes." "Does the organization employ measures to preserve cybersecurity of the CCS after a disruption or organizational incident?" Yes.

Go right to 26.8 and say, "Which of the following disaster measures does the organization have?" Once you choose from that list there you can specify a little easier, "How do you test the alternate site and how often do you test the alternate site?" It was similar to an earlier training tip. It just might help the flow if you jump to that and let them choose how they're going to do it first.

Alternate Site and Disaster Recovery: Training Tips –2

Clarification – Some organizations' continuity of operations plans may combine business continuity and/or disaster recovery plans. Check all that apply for an accurate CPRI.

Question 26.8
Which of the following disaster measures does the organization have? (*Check all that apply.*)

- ❑ Alternate-site operations include cybersecurity measures consistent with those in place for the original operational functions.
- ❑ Recovery/reconstitution phases include cybersecurity measures consistent with those in place for the original operational functions.
- ☑ Organization has continuity of CCS operations plans that include cybersecurity.
- ☑ Organization has CCS disaster recovery plans that include cybersecurity.
- ☑ Organization has business continuity plans that include cybersecurity.
- ❑ Organization has CCS backups of data and software available such that services can be restored quickly to an equivalently secure state.
- ❑ Organization has no documented measures.

Homeland Security

115

**115 Training Tip 2. Some organizations' continuity of operation plans may combine business continuity and/or disaster recovery plans. Check all that apply for a CPRI, for an accurate CPRI.

So they may think of basically, what we're trying to say here, is they may think of them one and the same but if they truly are doing one and the same, it offers two distinct possibilities here in the list, so organization has a continuity of critical service operation plans and also has a disaster recovery. Just be sure to give them credit, even if they combine the two concepts.

Alternate Site and Disaster Recovery: Training Tips –3

Clarification – When soliciting accurate answers for Question 26.8 (Incident Response), verify that the organization's plans for continuity of operations, disaster recovery, and/or business continuity explicitly include cybersecurity for the CS.

Question 26.8
Which of the following disaster measures does the organization have? (*Check all that apply.*)

- ❑ Alternate-site operations include cybersecurity measures consistent with those in place for the original operational functions.
- ❑ Recovery/reconstitution phases include cybersecurity measures consistent with those in place for the original operational functions.
- ❑ Organization has continuity of CCS operations plans that include **cybersecurity**.
- ❑ Organization has CCS disaster recovery plans that include **cybersecurity**.
- ❑ Organization has business continuity plans that include **cybersecurity**.
- ❑ Organization has CCS backups of data and software available such that services can be restored quickly to an equivalently secure state.
- ❑ Organization has no documented measures.

Homeland Security

116

**116 When soliciting accurate answers to Question 26.8, verify that the organization's plans for continuity of operations, disaster recovery, or business continuity explicitly includes cybersecurity for the critical service as well. So what I've seen sometimes is they'll bring in a disaster recovery team or business continuity team, but as we start asking them some questions, they're not considering cybersecurity, they're not considering some of the network assets, so when this happens, you kind of want to push them a little to see if they truly are thinking about cybersecurity aspects of that as well.

Cyber Dependencies

Table of Contents

Cyber Dependencies

Cyber Infrastructure Survey (CIS) Training Course

Homeland Security

117

**117 The last domain is Cyber Dependencies.

Cyber Dependencies Domain –1

This part of the survey assesses the dependency of the CS on data services/providers and the organization's continuity plans, which would be used in the event of a loss of those data services. Specifically, it assesses

- whether the organization uses internal and/or external communication providers in support of the CS,
- whether the organization has a contingency/business continuity plan in place for when data may be unavailable or service is lost,
- what type of data processing services are required for the operation of the CS, and
- whether the CS depends on endpoint systems (e.g., desktops and laptops).

**118 So we're going to look at whether the organization uses internal and/or external communication providers, whether the organization has a contingency or business continuity plan in place for when data may be unavailable, what types of data processing services are required, and whether the critical service depends on endpoint systems.

Cyber Dependencies Domain –2

Cyber Dependencies Domain	Checkbox	If Yes	Text Input	Notes	Total
Data at Rest	1	5		2	**8**
Data in Motion	2	18		2	**22**
Data in Process	1	8		2	**11**
Endpoint Systems	1	5		2	**8**
Total	**5**	**36**		**8**	**49**

This domain contains a total of **49** questions.

- There are 5 simple Checkbox responses.
- There are 36 If-Yes questions, which require an additional response if the parent question is answered “Yes.”
- There are 8 Notes questions.

Homeland Security

119

**119 Three, or the four, subdomains are going to be data at rest, data in motion, data in process.

Student: Bless you.

Instructor: Endpoint systems.

Data at Rest: Overview

Cyber Dependencies Domain	Checkbox	If Yes	Text Input	Notes	Total
Data at Rest	1	5		2	**8**

In Data at Rest, the goal is to assess

- whether data storage strategies are required for the CS and
- the impact to the CS if data storage becomes unavailable or service is lost.

**120 So in data at rest, we're going to assess whether the data storage strategies are required for the critical service and the impact to the critical service if data storage becomes unavailable or service is lost.

Data at Rest: Concepts and Terminology –1

Storage Area Network (SAN) – A dedicated high-speed network that interconnects and presents shared pools of storage devices to multiple servers (A SAN allows each server to access shared storage at a high speed as if it were directly attached to the server.)

Network Attached Storage (NAS) – A dedicated file storage device that provides local area network nodes with file-based shared storage (Each NAS resides on the LAN and has its own IP address.)

**121 Key concepts and terminology. So a Storage Area Network. A dedicated high-speed network that interconnects and presents shared pools of storage devices to multiple servers. Network Attached Storage. A dedicated file storage device that provides local area network nodes with file-based shared storage.

Data at Rest: Concepts and Terminology –2

Human Machine Interface (HMI) – The user interface and primary tool operators and line supervisors used to coordinate and control programmable logic controllers (PLCs) in support of industrial and manufacturing process control system(s)

Storage as a Service (SaaS) – A business model where a company leases or rents its storage infrastructure to another company or individuals

Best Practice

When access to stored data is required to support cyber operations, ensure there is a backup mode of communication in case the primary method for accessing the data is lost or becomes unavailable.

Homeland Security

122

**122 Human Machine Interface. Think that's self-explanatory. Storage as a Service.

So best practice. When access to stored data is required to support cyber operations, ensure there is a backup mode of communication in case the primary method for accessing the data is lost or becomes unavailable.

Data at Rest: Training Tips

Clarification – In Question 27.1, Subpart 3 (Cyber Dependencies) there should be a planned alternate mode or capability in the event of loss. The alternate mode does not need to be identical to the primary mode, but it must be planned.

Question 27.1, Subpart 3 Does the organization have alternative or backup storage capabilities that can be used in case of loss of the primary storage?	❑ No ❑ Yes

Homeland Security

123

**123 Training tip for Data at Rest. In Question 27.1, Subpart 3, there should be a planned alternate mode or capability in the event of a loss. The alternate mode does not need to be identical to the primary mode, but it must be planned. So does the organizations have alternate or backup storage capabilities that can be used in case of loss of the primary storage? It doesn't have to mirror the exact, the exact solution that you specified in the earlier parts. Just make sure they have a planned backup.

Data in Motion: Overview

Cyber Dependencies Domain	Checkbox	If Yes	Text Input	Notes	Total
Data in Motion	2	18		2	**22**

In Data in Motion, the goal is to assess whether

- external communications are required for the organization's CS and
- internal communications are required for the organization's CS.

Homeland Security

124

**124 Data in Motion. Assess whether external communications are required for the organization and whether internal communications are required for the organization's critical service.

Data in Motion: Concepts and Terminology

Telecommunications (Telecom) Service Provider – A service provider that provides telephony and data communications services (These services may include local exchange carriers and mobile wireless communications.)

Best Practice

Monitor external and internal communications. Identify and document communication services that the CS relies on. Use an active notification system (i.e., phone call, email, or text message) that supplies alerts when services are unavailable.

125

**125 So Telecom service provider. A service provider that provides telephony and data communications services. These services may include local exchange carriers and mobile wireless communications.

So best practice. Monitor external and internal communications. Identify and document communication services that the critical service relies on. Use an active notification system such as phone call, email, text message, that supplies alert when services are unavailable.

Data in Motion: Training Tips –1

Clarification – In Question 28.1 (Cyber Dependencies) Telecom provider refers to a communications service provider that provides telephone and similar (or related) services (e.g., voice circuits for modem pools)

Question 28.1 If yes, who/what is the dependency on?	❑ Networking provider ❑ Telecom provider

126

**126 Training Tip 1 for Data in Motion. In Question 28.1, Telecom provider refers to a communications service provider that provides telephone and/or similar services, such as voice circuits for model pools. So we have if/yes, who/what is the dependency on? One of the things is Telecom provider. We're looking for someone that provides telephone services or voice circuits for modem pools, so if you're at a energy utility or somewhere with some remote sites, that could be a dependency that you may want to push them on to see if they have identified and see if it's an accurate response here.

Student: So if it's voiceover--

Student: So if they're using point-to-point cellular service for their substations back to their ICS system? That's what we're looking for here. That would not be considered network provider? Would be a Telecom provider?

Instructor: Yeah. I would think if that point-to-point network is leased out through someone, is what we would be looking for here.

Instructor: Yeah. So there's, there's some overlap in some of this, right? Which is what we saw also. In this instance, what, you know, some of those may be acting basically as a network provider, right. This is actually using telephony services for some of this and that's, that's why the distinction.

Student: So if you have a voiceover IP, you don't mark that Telecom, you don't put a network provider, in the Telecom provider's box.

Instructor: No. So depending upon how--

Student: Okay.

Instructor: --voiceover IP's being used for the service support, right, so the example given to us is just like what you see here, or you'll still see in use, like, general Telecom circuits, right, but being used to run, like, modem pools.

Student: Mm-hm.

Instructor: Because that's how they're communicating, right. So not necessarily a data communications service, but something that's really a telephony-based service that's still in use.

Data in Motion: Training Tips –2

Data in Motion: Training Tips –2

Clarification – Answer all time intervals in Question 28.1, Subpart 9 (Cyber Dependencies) as whole units. For example, if an answer is "1.5 hours," enter "90 minutes," or if an answer is "2.5 days," answer "60 hours."

Question 28.1, Subpart 9 Once the primary mode is restored, how long will it take before full resumption of operations?	_____ Minutes (enter the number of minutes) _____ Hours (enter the number of hours) _____ Days (enter the number of days)

Homeland Security

**127 All right. Training Tip 2. Answer all time intervals in Question 28.1, Subpart 9, as whole units. For example, if an answer is "one and a half hours," enter "90 minutes," or if an answer is "two and a half days," answer "60 hours."

Again, earlier training tip, use whole numbers instead of date ranges or increments.

Instructor: All right. And this is important. This was stressed to us multiple times. They want to see whole numbers here. I believe it's for a particular reason, but you don't want to use fractional values.

Student: What about values?

Instructor: No. Single value. So if it's, you know, if you're going to tell me, like here, two and a half days--

Student: That's what I'm saying. That could be 2 days and 12 hours.

Instructor: Yeah. So no. It's going to get converted to just hours. Right. Just like if you're going to tell me, you know, one and a half hours, I want to convert it to 90 minutes, right? That's what they're after.

Data in Process: Overview

Cyber Dependencies Domain	Checkbox	If Yes	Text Input	Notes	Total
Data in Process	1	8		2	**11**

In Data in Process, the goal is to assess the

- dependence of the CS on data processing services and
- ability of the CS to absorb the loss of data processing services.

**128 All right. Data in Process. So the goal is to assess the dependence of the critical service on data processing services and the ability of the critical service to absorb the loss of data processing services.

Data in Process: Concepts and Terminology –1

Mainframe – A high-speed computer that supports large critical applications, numerous workstations, and network peripherals

Server Cluster – A group of linked servers, working in coordination and deployed to improve performance and/or availability over and above that provided by a single server

**129 So some concepts and terminology, mainframe, server cluster. A group of linked servers, working in coordination and deployed to improve performance and/or availability over and above that provided by a single server.

Data in Process: Concepts and Terminology –2

Cloud Provider – A company that owns and offers network services, infrastructure services, or business applications from a remote location to other businesses or individuals

Best Practice

Monitor data processing services. Use an active notification system that provides an alert when a service becomes unavailable. If an outside vendor is used to provide and/or support this service, ensure that the contingency/ business continuity plan includes the requirements and limitations imposed by a contract or service level agreement.

**130 Cloud provider.

So best practice for this subdomain would be monitor data processing services. Use an active notification system that provides an alert when a server, service, becomes unavailable. If an outside vendor is used to provide and/or support the service, ensure that the contingency business continuity plan includes the requirements and limitations imposed by a contract or service level agreement.

Endpoint Systems: Overview

Cyber Dependencies Domain	Checkbox	If Yes	Text Input	Notes	Total
Endpoint Systems	1	5		2	**8**

In Endpoint Systems, the goal is to assess the CS for its

- dependence on IT systems such as desktop, laptop, and tablet computers and
- ability to absorb the loss of endpoints.

**131 Endpoint Systems. We're going to assess the dependence on IT systems such as desktop, laptop and tablet computers and the ability to absorb the loss of the endpoints in this subarea.

Endpoint Systems: Concepts and Terminology –1

Programmable Logic Controller (PLC) – A digital computer typically used for automating industrial electromechanical processes, such as control of machinery on factory assembly lines, amusement rides, or light fixtures (PLCs are used in many industries.)

Industrial Control System (ICS) – Integrated hardware and software designed to monitor and control the operation of machinery and associated devices in industrial environments

Supervisory Control and Data Acquisition (SCADA) – A category of software applications used for process control that gathers data in real time from remote locations to control equipment and conditions (SCADA systems are used in power plants, as well as oil and gas refining, telecommunications, transportation, and water and waste control, etc.)

132

**132 So key terminology here is Programmable Logic Controller, Industrial Control System, Supervisory Control and Data Acquisition, SCADA. You'll see, you'll sometimes out on the field see these two terms interchanged. From what I've seen, the SCADA systems focus really on a larger operating path. If there's some remote sites, Industrial Control Systems are normally categorized as using the PLCs and stuff, but it could be over big distances or it could be self-contained systems. But it seems to be the distinction for SCADA is over to remote sites and kind of longer hauls.

Endpoint Systems: Concepts and Terminology –2

Business Continuity Plan – Documentation of predetermined instructions or procedures that describe how an organization's mission/business functions will be sustained during and after a significant disruption

Best Practice

When endpoint systems are required to operate the CS, identify the impact to the CS if one of these systems fails or is unavailable. Establish a business continuity plan for restoring CS endpoints within an acceptable amount of time.

Homeland Security

133

**133 Business Continuity Plan. So best practice. When endpoint systems are required to operate the critical service, identify the impact of the critical service if one of these systems fails or is unavailable. Establish a business continuity plan for restoring endpoints within an acceptable amount of time.

Question Intent: Objectives Summary

In this section, for each domain, you learned

- concepts and terminology,
- training tips,
- about QA (e.g., know to watch for inconsistent responses),
- best practices, and
- how different areas of the survey support each other.

Homeland Security

**134 So in summary, we've gone through all the concepts and terminology required for each of the domains and the subdomains. We've provided training tips, talked about different QA checkpoints, applied best practices and how different areas of the survey support each other, and that ends this section.