RECEIVED
JUN 14 2021

LABOR RELATIONS

UNITED STATES POSTAL SERVICE

June 11, 2021

Mr. Brian Wagner
President
National Association of Postal Supervisors
1727 King Street, Suite 400
Alexandria, VA 22314-2753

Certified Mail Tracking Number
7018 0360 0001 6256 7158

Dear Mr. Wagner:

The Postal Service plans to administer a new training course to all employees with computer access. Two versions of this course have been created, one for bargaining unit employees and one for all other employees. The purpose of these courses it to educate employees of their responsibilities under the Privacy Act.

When implemented, all employees with computer access will be required to complete this course through HERO within 90 days of being assigned the course. Any employee who fails to complete the course within 90 days will have his/her computer access restricted until the course is completed.

We have enclosed a copy of both versions of the course and a document detailing its content and purpose.

Please contact Bruce Nicholson at 7773 if you have questions concerning this matter.

Sincerely,

David E. Mills
Director
Labor Relations Policies and Programs

Enclosures

475 L'ENFANT PLAZA SW
WASHINGTON DC 20260-4100
WWW.USPS.COM

ETHICS & LEGAL COMPLIANCE
LAW DEPARTMENT

UNITED STATES POSTAL SERVICE

To: David Mills, Director, Labor Relations Policies and Programs

From: Janine Castorina, Chief Privacy and Records Management Officer

Re: Privacy Compliance Training

The Privacy Act of 1974 governs how the Postal Service deals with personally identifiable information (PII). 5 U.S.C. section 552a. Congress set out how the Postal Service can gather PII, use it, how it must protect it, and how it can disclose it. 5 U.S.C. section 552a(e). The Postal Service's responsibilities flow down through its employees, contractors and vendors. 5 U.S.C. section 552a(m).

The information covered by the Privacy Act is vast and covers any personally identifiable information that is a record and it is covered in a system of records. 5 U.S.C. section 552a(a)(4). A Privacy Act record is any item or collection of items, that are about an individual, "including, but not limited to, his education, financial transactions, medical history, and criminal or employment history," which contains a name or other identifying particular by which an employee can be identified. 5 U.S.C. section 552a(a)(4). A system of record, is a legal construct, describing how the Postal Service searches and categorizes its records. 5 U.S.C. section 552a(a)(5). Based on these definitions, it is clear that most of the Postal Service's data and computer systems are covered by the Privacy Act. Some limited examples include the TACS system, COA, and collection of information from individuals submitting Passport applications, among others.

Once it is determined that data is covered by the Privacy Act, the statute directs that the Postal Service protect that data by "establish[ing] appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records." 5 U.S.C. 552a(e)(10). Examples of administrative safeguards include implementation regulations (such as the CFR, the ELM and the Handbook AS-353), training, and other measures that set out the requirements of the Privacy Act and inform employees how to meet those requirements.

Informing employees, through training and other means, how to meet the Privacy Act's requirements is particularly important, because the Privacy Act, unlike other statutes, the Privacy Act provides for not only civil remedies against the Postal Service for failure to comply with the Act, but also provides for criminal penalties for "[a]ny officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information... and who

475 L'ENFANT PLAZA SW
WASHINGTON, DC 20260-4201

knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it." 5 U.S.C. sections 552a(g)(1) and (i)(1).

Accordingly, the Postal Service has created a mandatory web-based training course – Privacy Act Compliance – for all employees with ACE IDs, and therefore, computer access. The purpose of this training course is to educate employees of the principles outlined above through three modules that help employees understand: 1. the Privacy Act and how it applies to them; 2 the "need to know" concept, so that they can avoid inadvertent disclosures that might violate the Privacy Act; and 3. when new initiatives must undergo a privacy review so that new projects can be completed within reasonable timeframes, while also being legally compliant. Once implemented, employees will have 90 days to complete the course. Failure to complete the course by the allotted time will result in partial revocation of employee computer access, which may only be restored by completion of the course.

Employees without computer access will be provided similar information, as applicable, through a variety of measures, including USPS TV rendition of the Privacy Act Compliance training, a DVD version of the Privacy Act Compliance training, and stand-up talks.

Janine Castorina

Digitally signed by Janine Castorina
Date: 2021.06.10 15:06:55 -04'00'

Janine Castorina

Chief Privacy and Records Management Officer

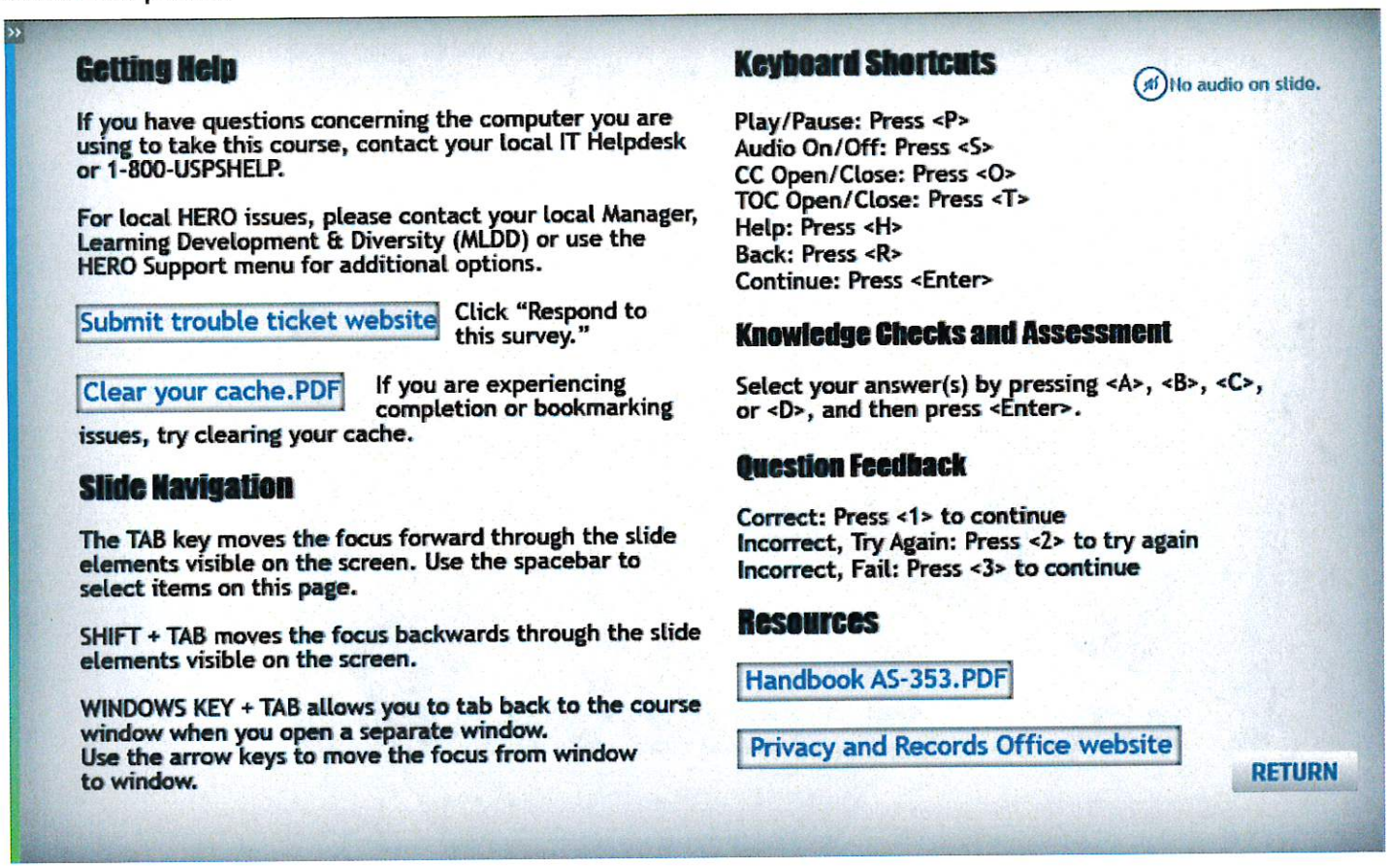
475 L'ENFANT PLAZA SW

WASHINGTON, DC 20260-4201

Slide 1 - Slide 1

Slide notes

Slide 2 - Help Menu



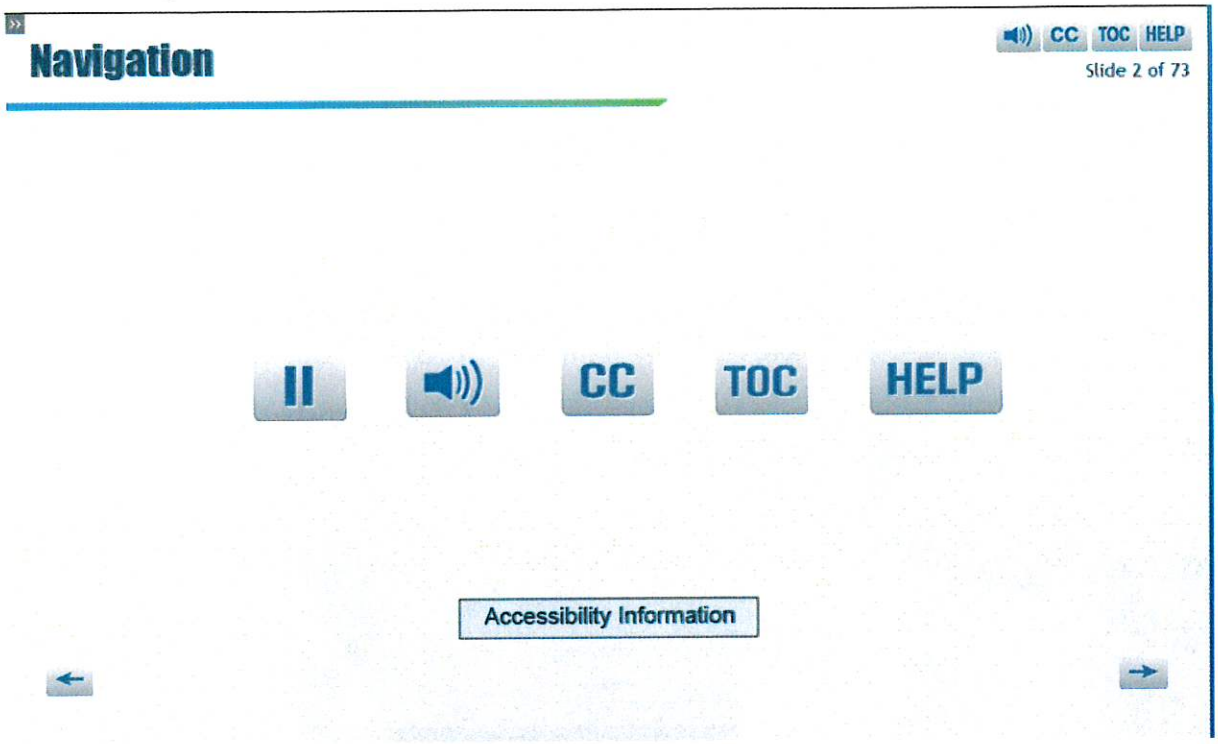
Slide notes

Slide 3 - Welcome

Slide notes

Welcome to the Privacy Act Compliance training course.

Slide 4 - Navigation



Slide notes

To navigate the course, the Play/Pause button allows you to pause then resume playing when you are ready.

Use the Audio button to mute or unmute audio.

The CC button turns Closed Captioning on or off, and the TOC button toggles the Table of Contents open or closed.

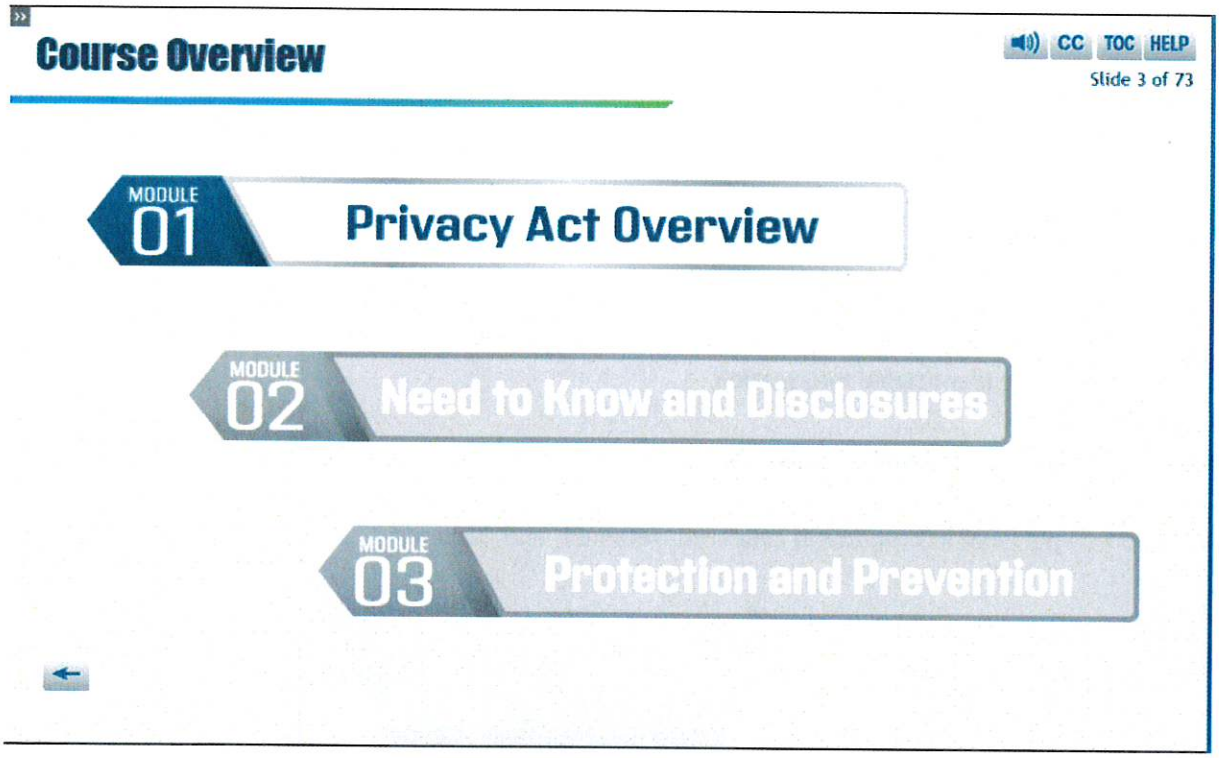
The Help button opens a screen with keyboard navigation shortcuts, troubleshooting information,

and links to resources mentioned in the course.

Use the Back arrow to return to the previous slide and the Forward arrow when you are ready to advance the course.

If you're using a screen reader, click the Accessibility Information button to learn more.

Slide 5 - Course Overview



Slide notes

This course aims to improve your familiarity with requirements of the Privacy Act, responsibilities for compliance,

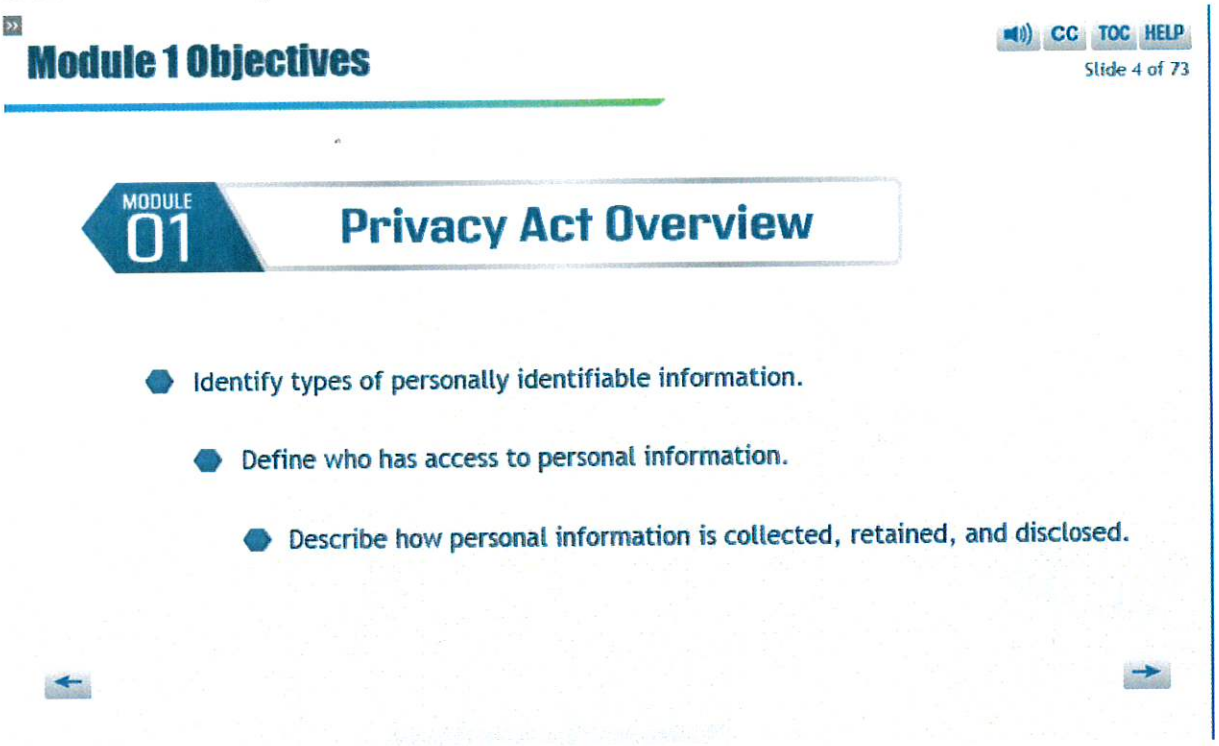
and implications of noncompliance in the Postal Service workplace.

We'll define a few key terms, examine several scenarios,

and then finish with strategies you can use to safeguard and maintain the security of personal information.

To get started, click the Module 1 tile.

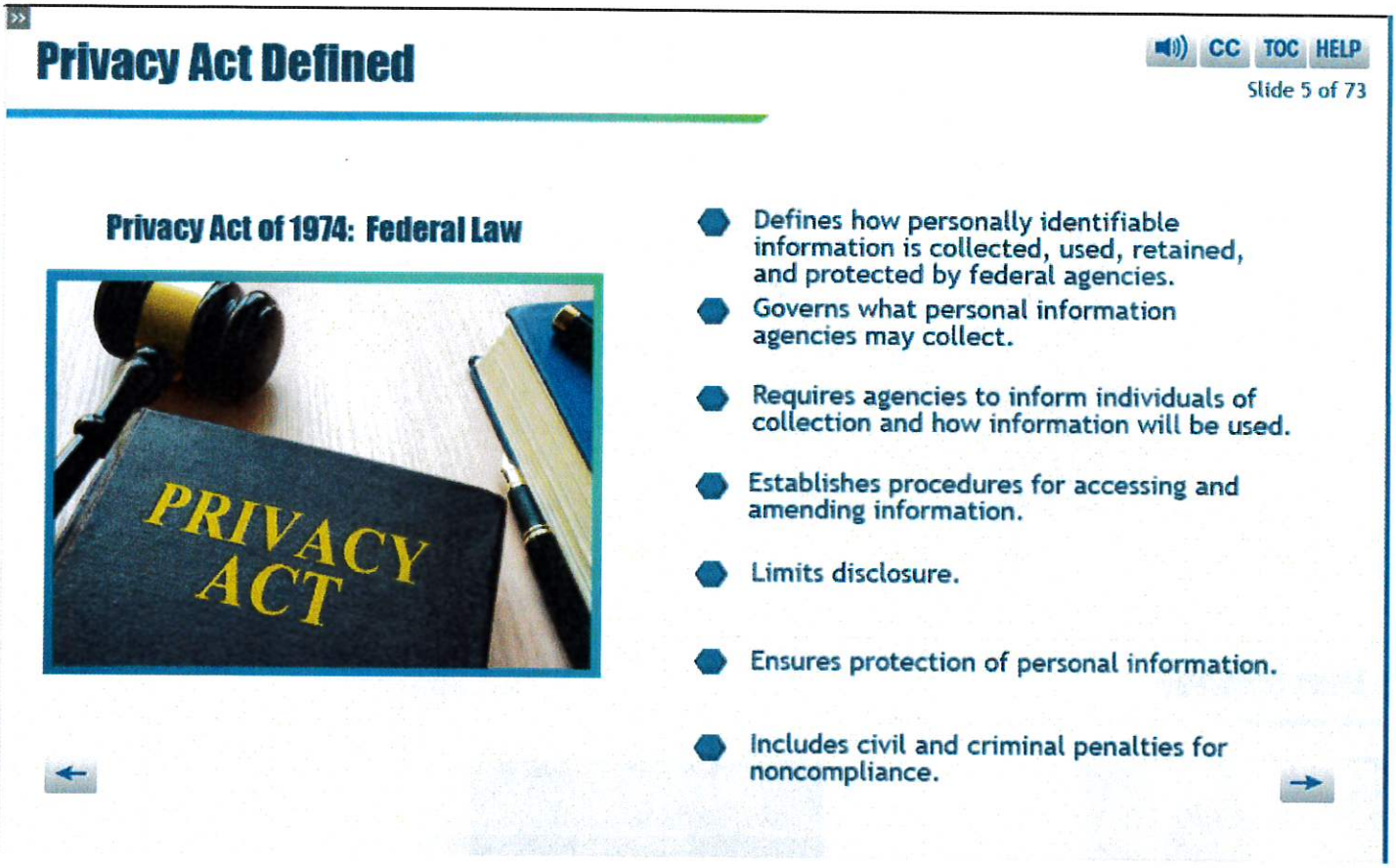
Slide 6 - Module 1 Objectives



Slide notes

Welcome to Module 1, Privacy Act Overview. By the end of this module, you should be able to identify types of personally identifiable information, define who has access to personal information, and describe how personal information is collected, retained, and disclosed.

Slide 7 - Privacy Act Defined



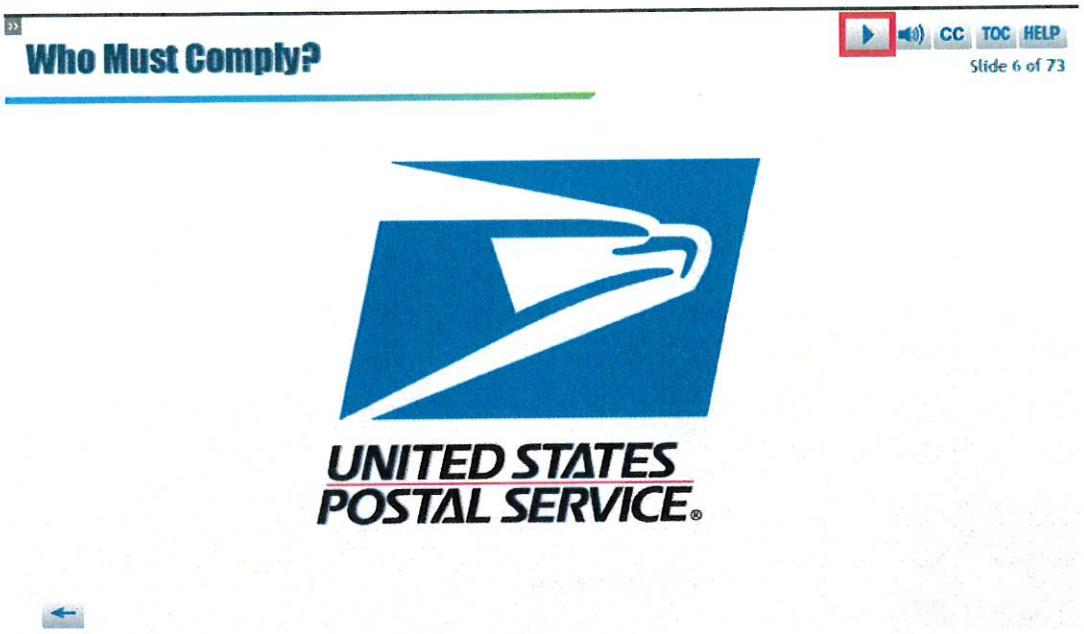
Slide notes

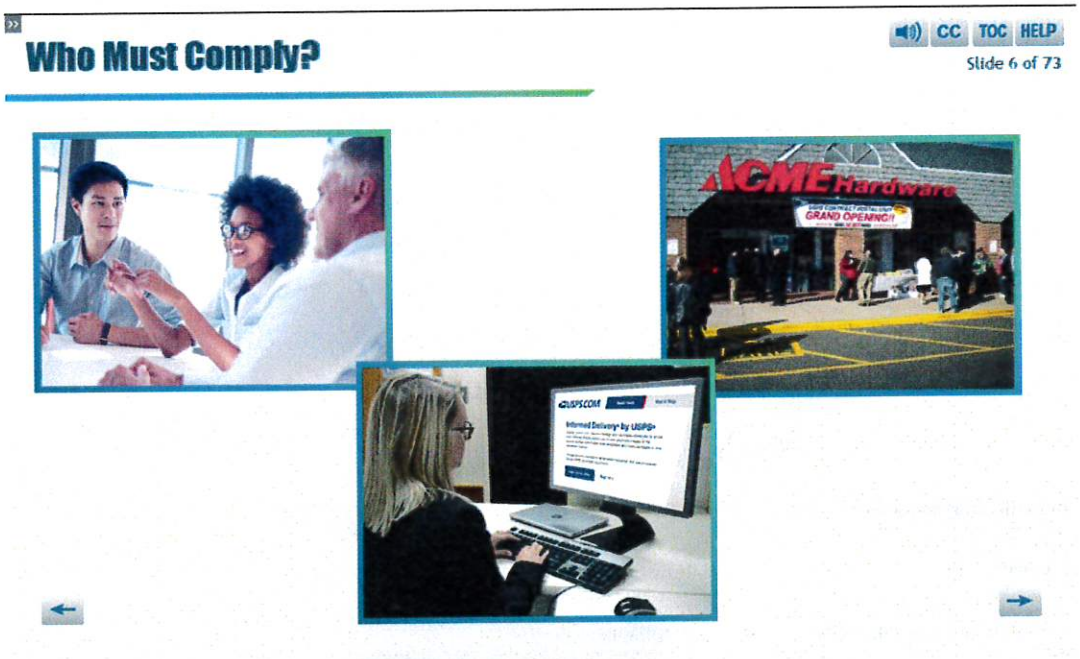
Let's start by defining our topic.

The Privacy Act of 1974 is a federal law that defines how personally identifiable information is collected, used, retained, and protected by federal agencies. The act governs the personal information agencies may collect and requires agencies to inform individuals of the collection and also how their information will be used.

The act establishes procedures for an individual to access and amend their information, limits disclosure, ensures protection of the information, and includes civil and criminal penalties for noncompliance.

Slide 8 - Who Must Comply?





Slide notes

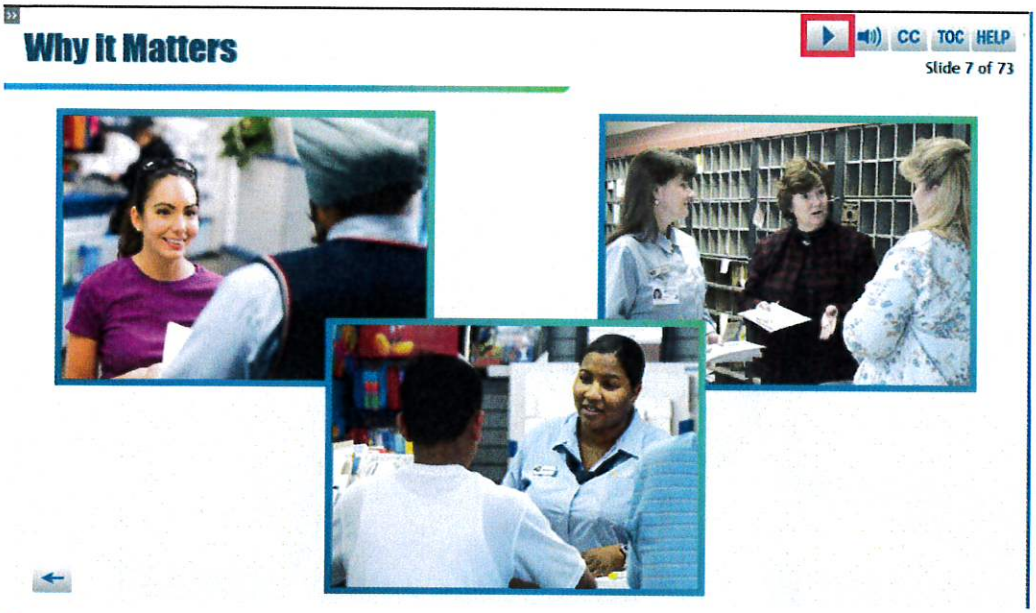
The Privacy Act applies to federal agencies in the public sector, including USPS, but does not apply to businesses in the private sector.

However, agents, contractors, and suppliers who help build or conduct USPS business operations,

and who have access to customer, employee, or other individuals' information,

must also abide by the Privacy Act and USPS privacy policies.

Slide 9 - Why it Matters



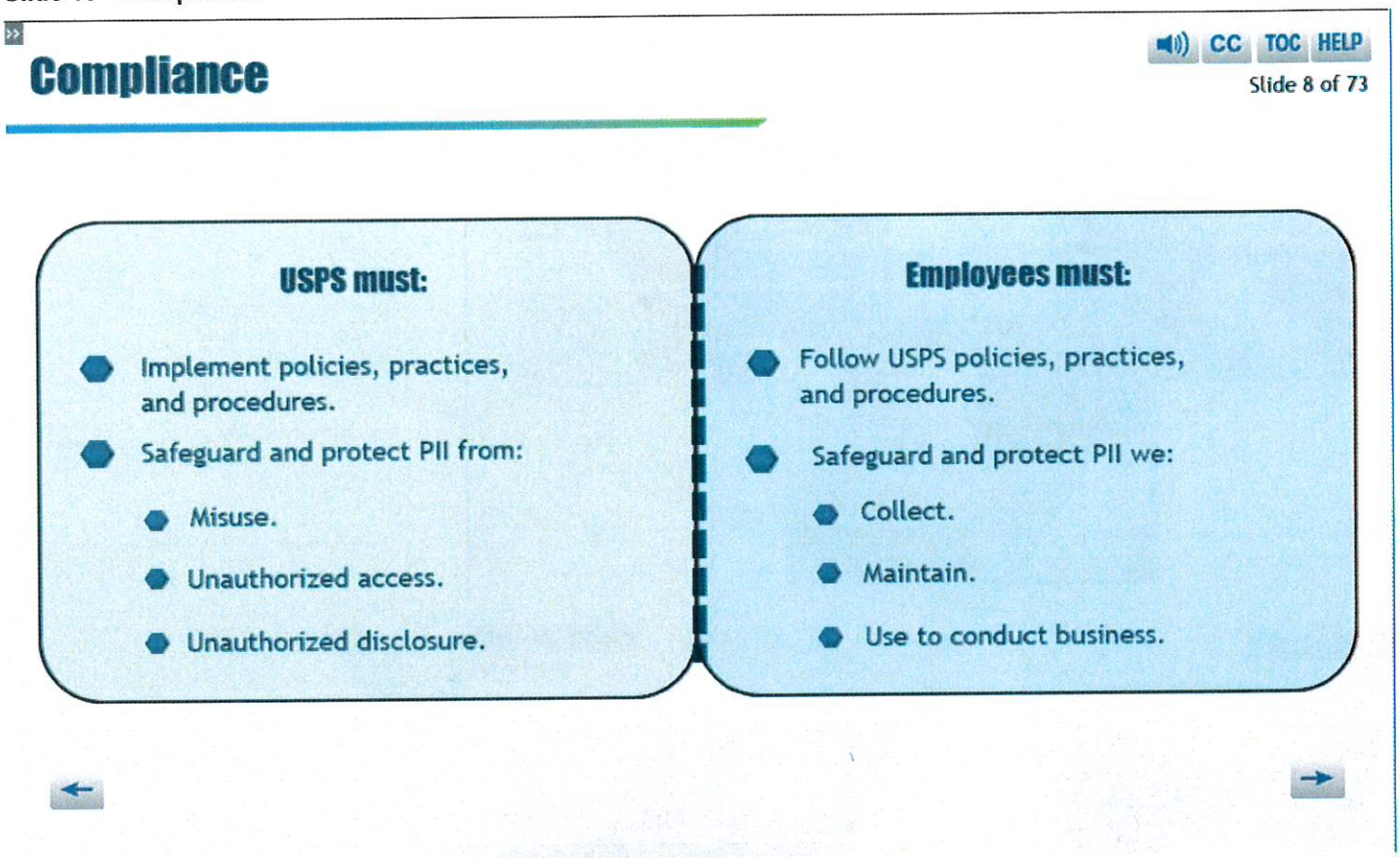
Slide notes

You may be wondering, why does the Privacy Act matter to me?

It matters because as a USPS employee, you play an important role in safeguarding the confidentiality and integrity of personal information.

Customers and employees depend on USPS as a trusted brand to protect the personal information they have agreed to share with us.

Slide 10 - Compliance



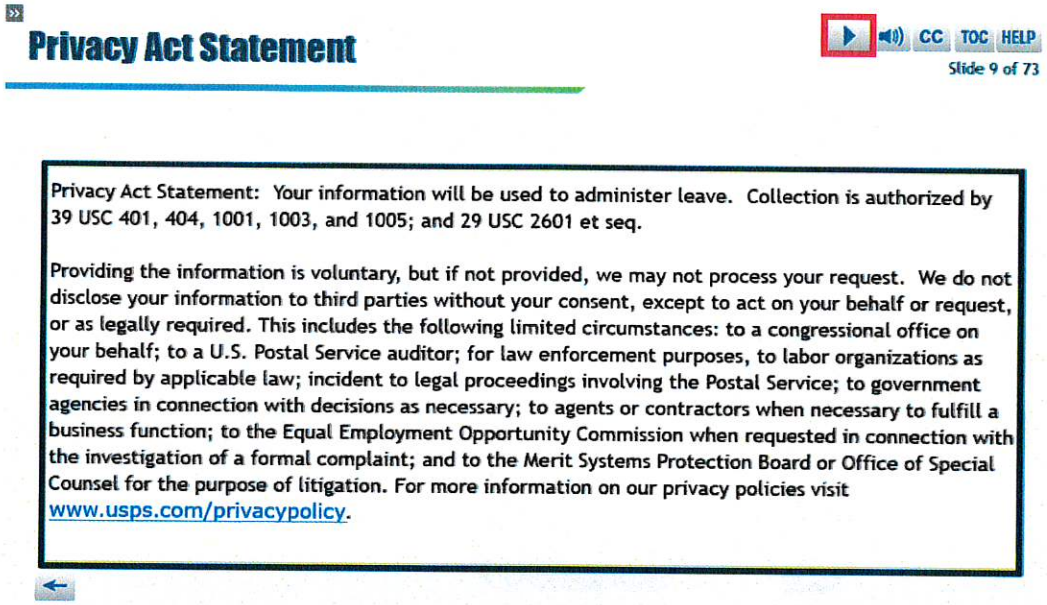
Slide notes

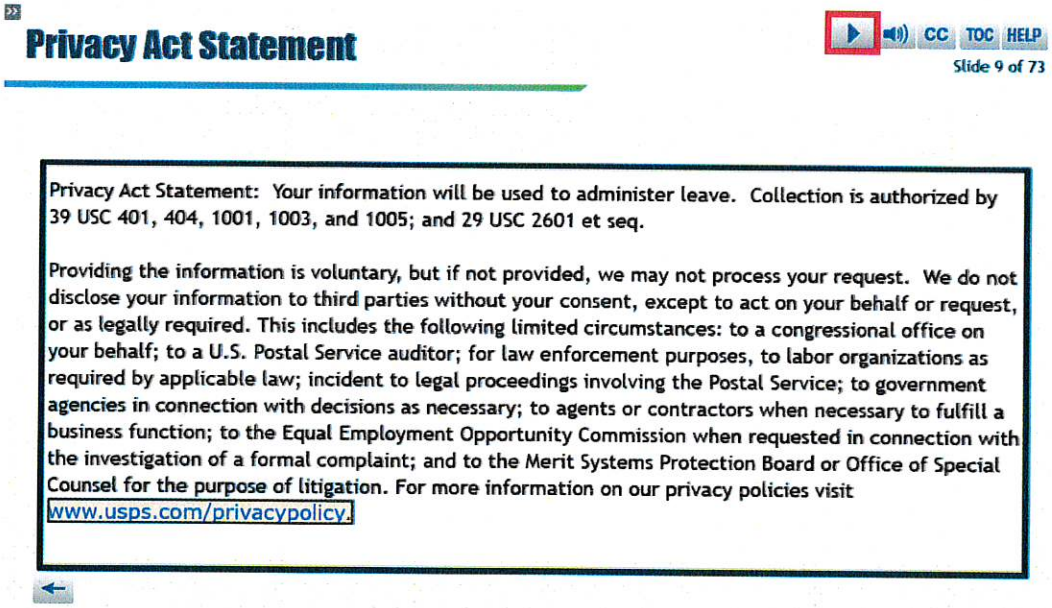
Now are you wondering how to comply?

First, USPS must implement policies, practices, and procedures to safeguard and protect personal information from misuse, unauthorized access, and unauthorized disclosure.

Second, all USPS employees, including you, must follow established USPS policies, practices, and procedures to safeguard and protect the PII we collect, maintain, and use to conduct business.

Slide 11 - Privacy Act Statement





Slide notes

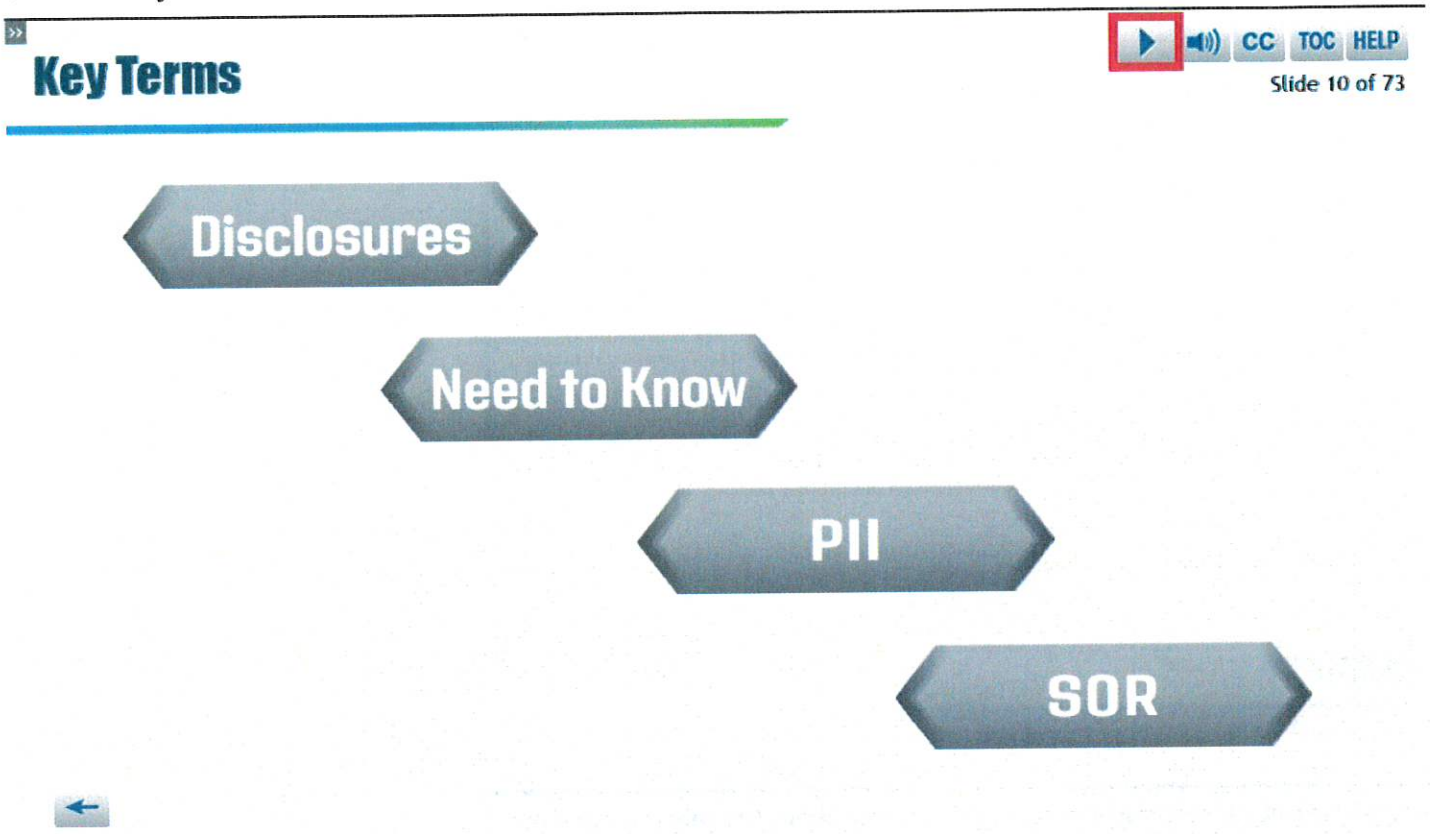
When a customer, employee, or other individual submits personal information to USPS,

we must provide a Privacy Act Statement, which includes a link to the USPS privacy policy.

This ensures the individual can make an informed decision on whether to share personal information

and informs them of USPS compliance to Privacy Act requirements.

Slide 12 - Key Terms



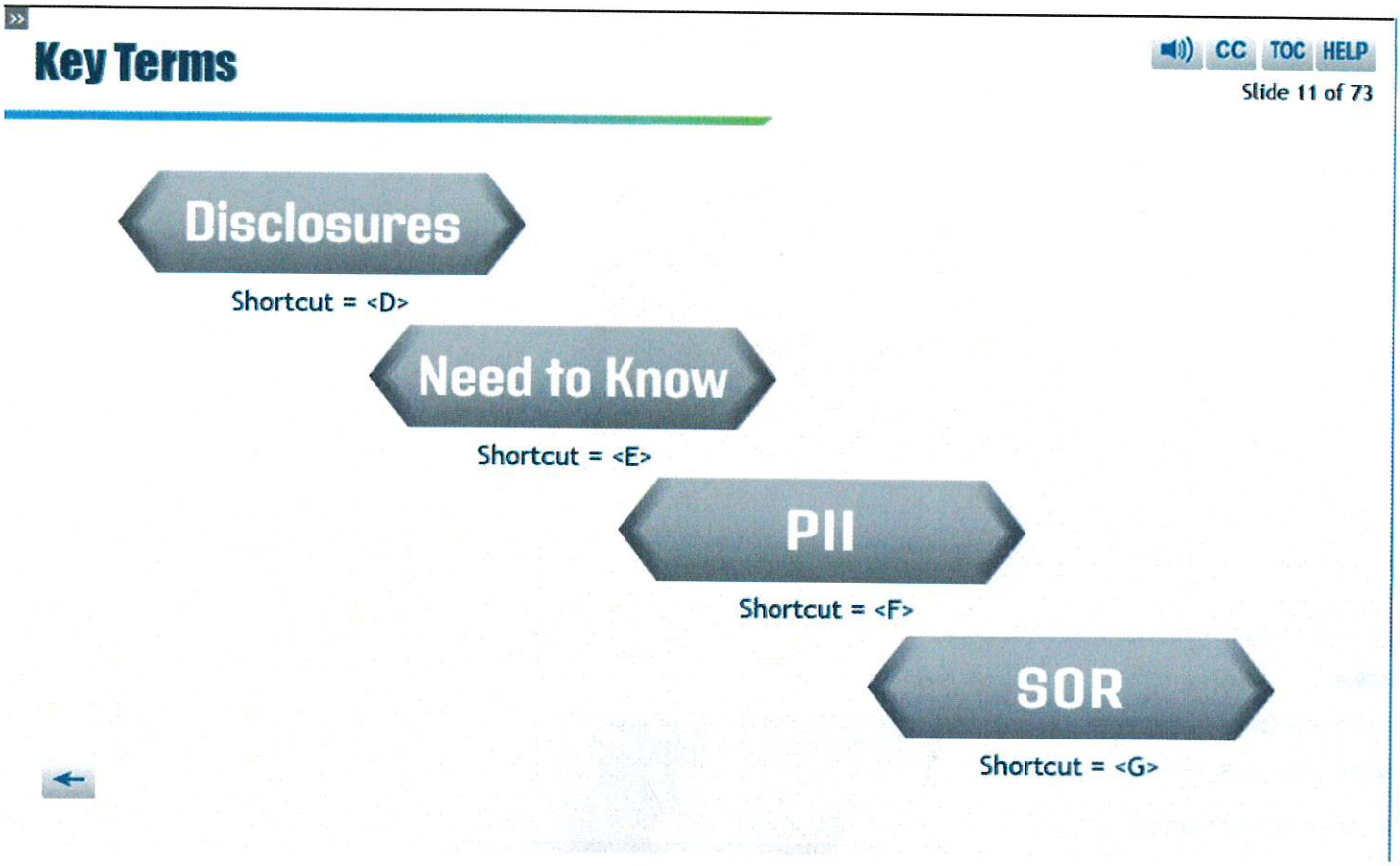
Slide notes

Now that you have a general idea of what the Privacy Act means to you as a USPS employee,

let's review a few key terms that will be used throughout the course.

For a description of each term, select the tiles.

Slide 13 - NOT IN TOC



Slide notes

Slide 14 – Disclosures

Disclosures

CC TOC HELP
Slide 12 of 73

Definition:

- The release of personal information:
  - Internally - within USPS
  - Externally - to third parties

Disclosures

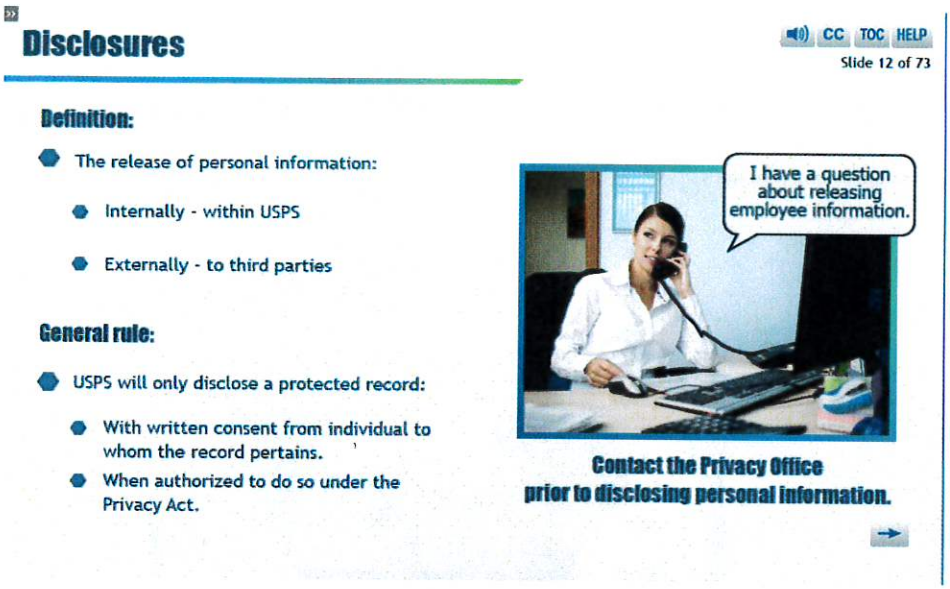
CC TOC HELP
Slide 12 of 73

Definition:

- The release of personal information:
  - Internally - within USPS
  - Externally - to third parties

General rule:

- USPS will only disclose a protected record:
  - With written consent from individual to whom the record pertains.
  - When authorized to do so under the Privacy Act.



Slide notes

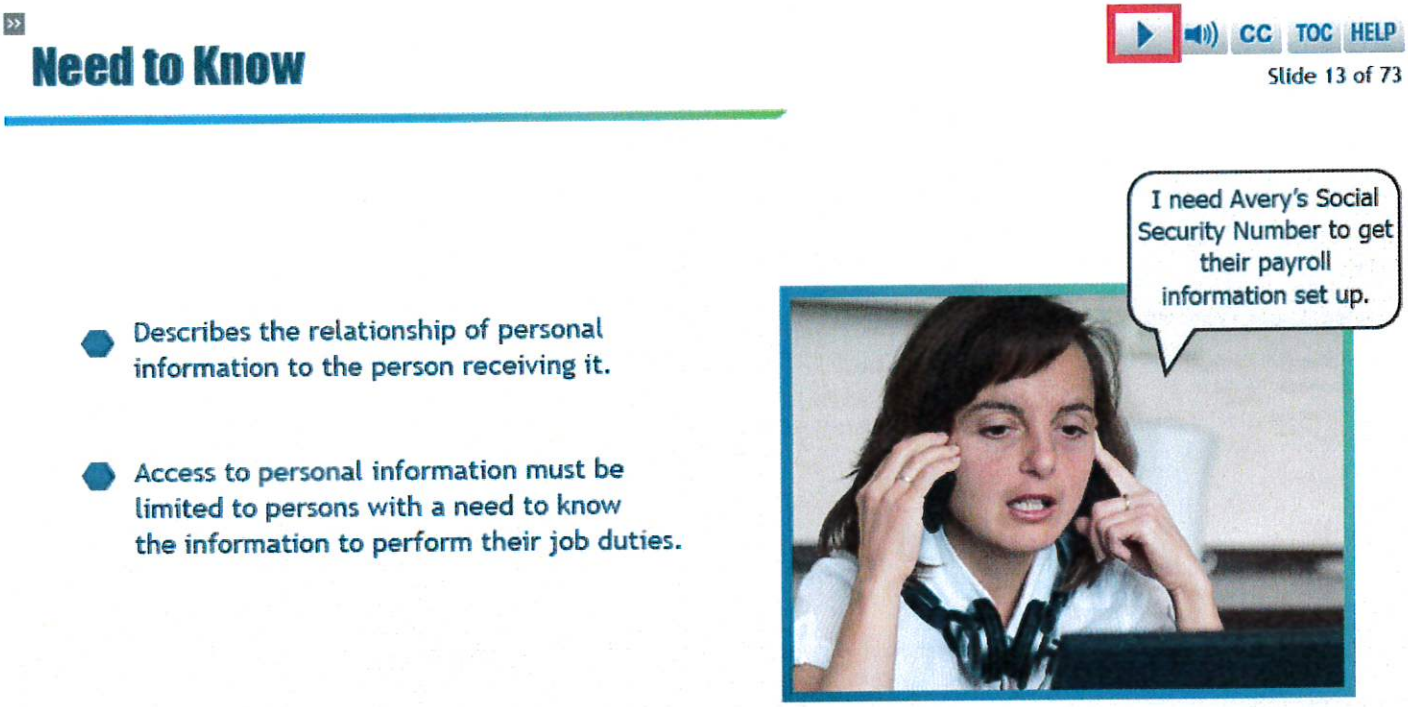
A disclosure is the release or sharing of personal information and can be made internally or externally, if authorized.

The general rule is that USPS will only disclose a record with written consent from the individual

or when authorized to do so under the Privacy Act.

Before making a decision about what information may be disclosed, consult the Privacy Office or Law Department.

Slide 15 - Need to Know



Slide notes

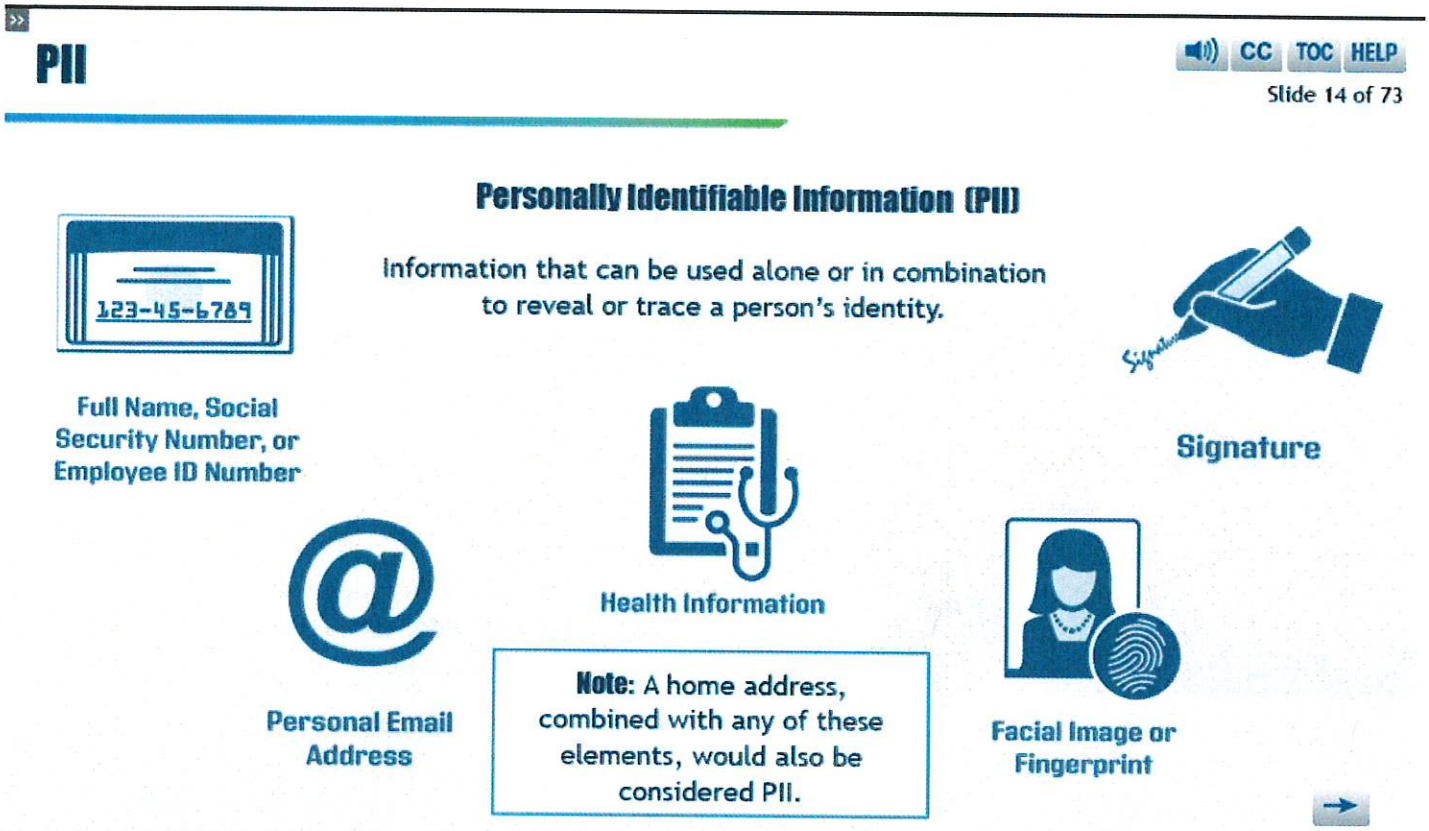
Need to know describes the relationship between information and the person receiving it.

Access to personal information must be limited to persons with a need to know the information to perform their job duties.

For example, an employee entering payroll information has a need to know the personal information of employees within their office,

but not the information for employees in a different office.

Slide 16 - PII



Slide notes

Personally Identifiable Information, or PII, is any information that can be used alone or in combination to reveal or trace a person's identity.

Examples of recognizable PII include a person's full name, Social Security Number, Employee Identification Number, or EIN,

personal email address, individually identifiable health information, a facial image, fingerprints, and an individual's signature.

While a home address alone is not PII, when it's combined with other identifying information,

such as a name, the address and name combined becomes PII.

Slide 17 - System of Records

System of Records

CC TOC HELP
Slide 15 of 73

System of Records (SOR)

- Formal legal concept defined in the Privacy Act
- Describes the way personally identifiable information is collected, used, maintained, and disclosed
- File, database, or program from which personal information is retrieved
- Not a physical location

Slide notes

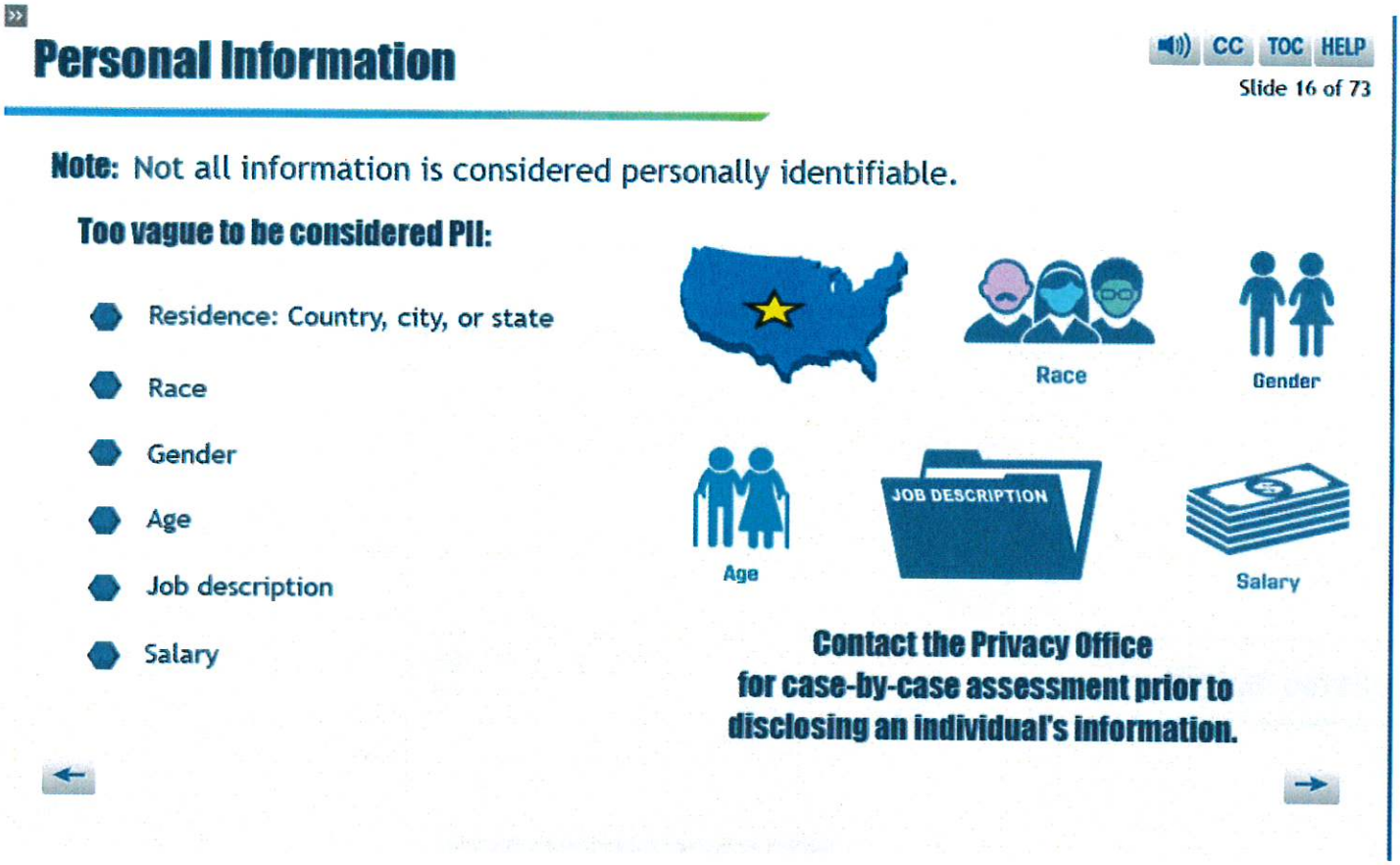
A System of Records, or SOR, is a formal legal concept defined in the Privacy Act

that describes the way personally identifiable information is collected, used, maintained, and disclosed.

A Privacy Act System of Records is a file, database, or program from which personal information is retrieved

and is not a physical location, such as a server or file cabinet.

Slide 18 - Personal Information



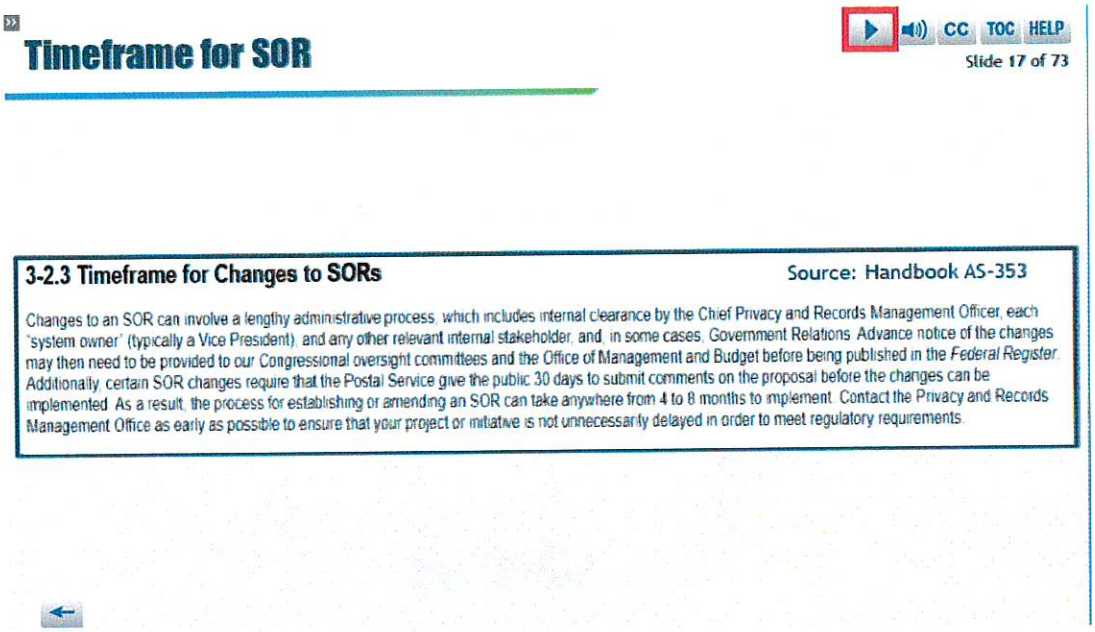
Slide notes

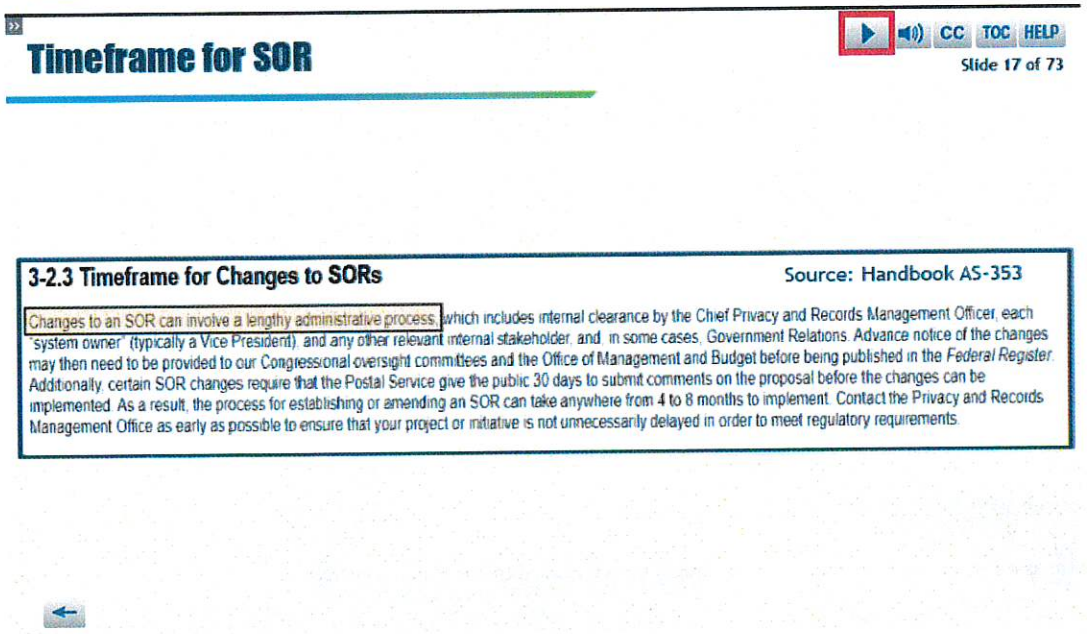
It's important to note, not all information pertaining to an individual is considered personally identifiable.

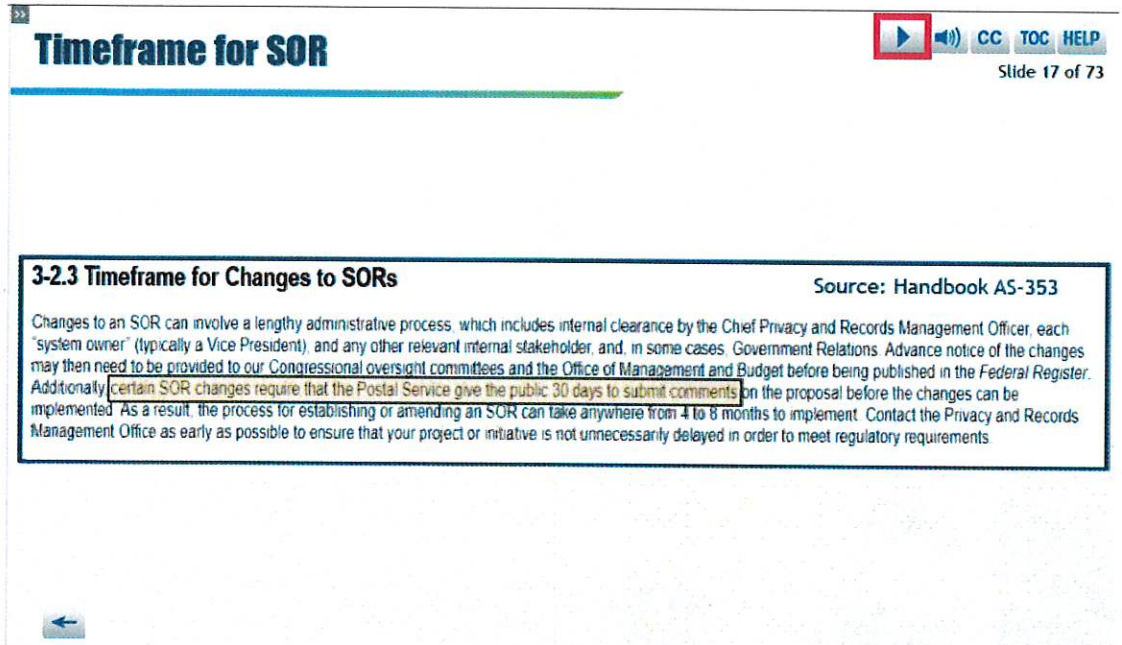
Some information is too vague to be linked to an identity. General residence information, such as a country, city, or state would not be considered PII by itself. Additionally, referring to a race, gender, age group, job description, or salary would not necessarily reveal someone's identity.

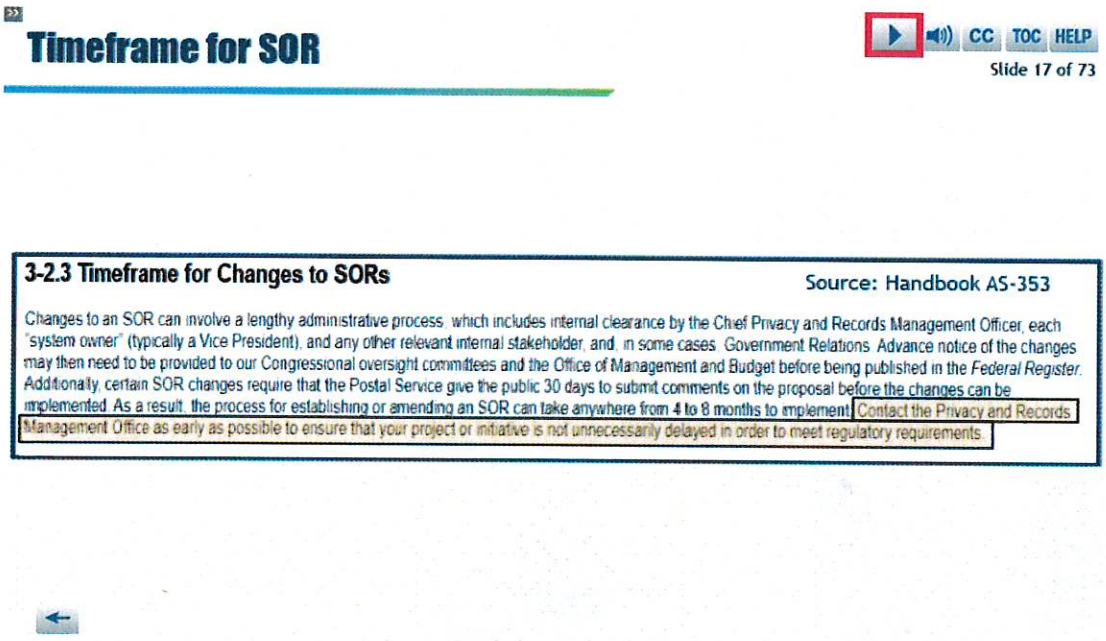
Whether something is PII requires a case-by-case assessment of the specific risk and should be determined by the Privacy Office.

Slide 19 - Timeframe for SOR









Slide notes

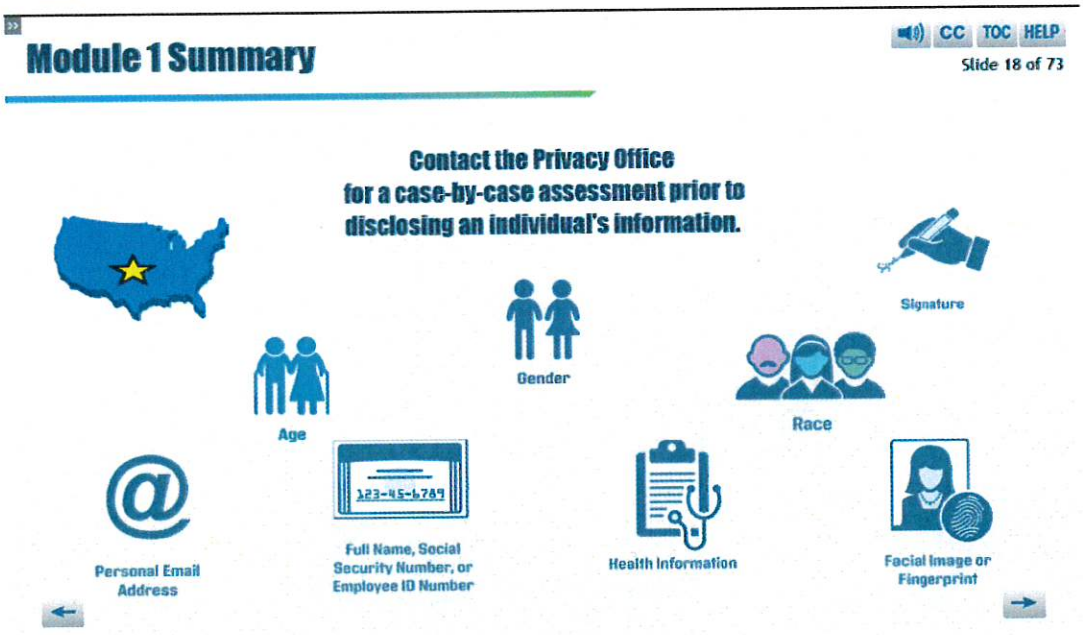
You learned the definition of an SOR, but it's important that you understand the timeframe associated with changes.

The creation or revision of an SOR is a multi-step process with mandatory time allotments for each item,

including a 30-day public comment period. You can expect the process to take 4 to 8 months to implement.

Make sure to contact the Privacy Office very early in the planning phase of any project that requires the collection of PII.

Slide 20 - Module 1 Summary



Slide notes

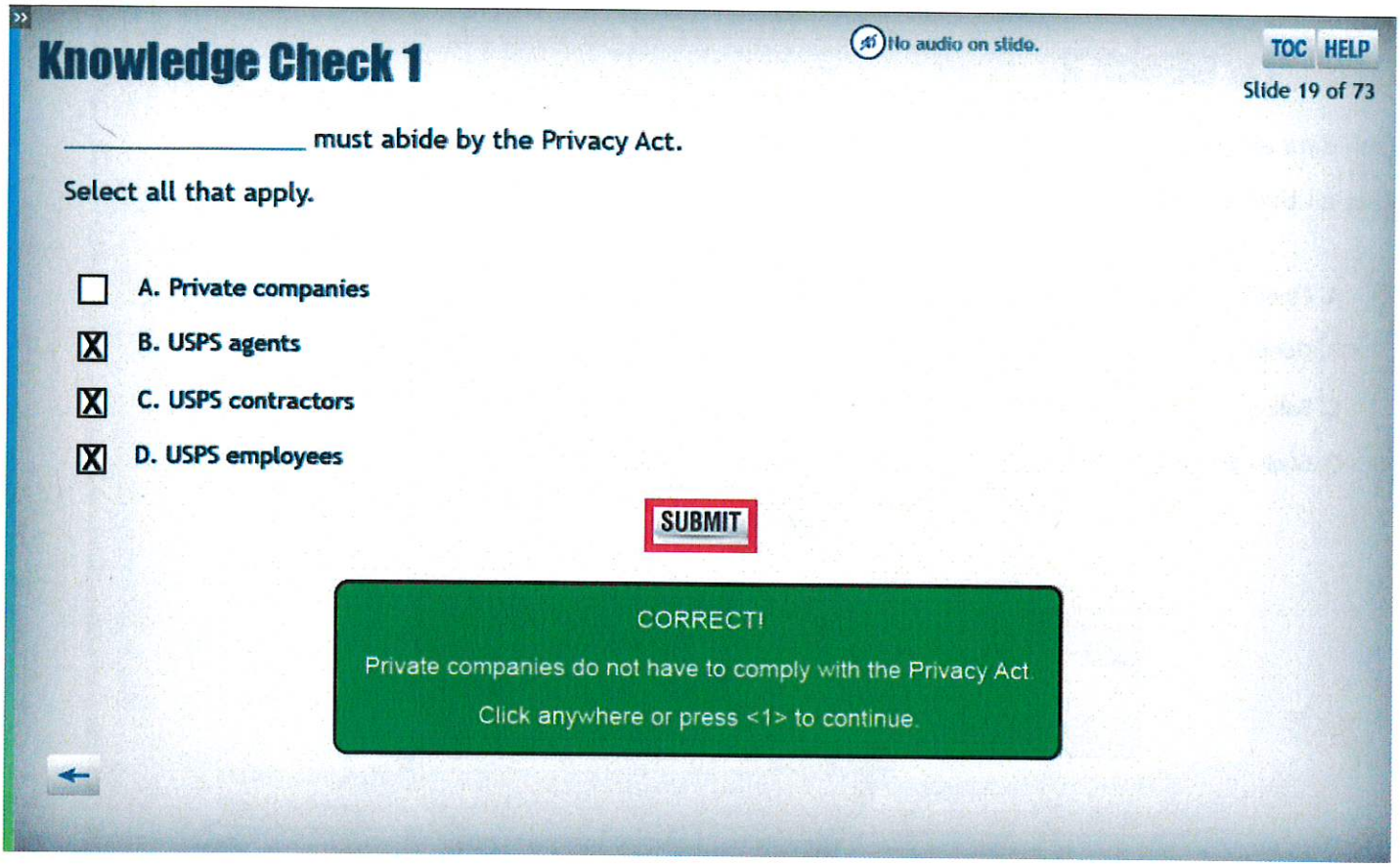
To review, USPS employees, agents, suppliers, and contractors are subject to privacy protection requirements of the Privacy Act.

Since it's often difficult to understand when information should be considered PII,

and because violations of the Privacy Act can lead to disciplinary action, up to and including termination,

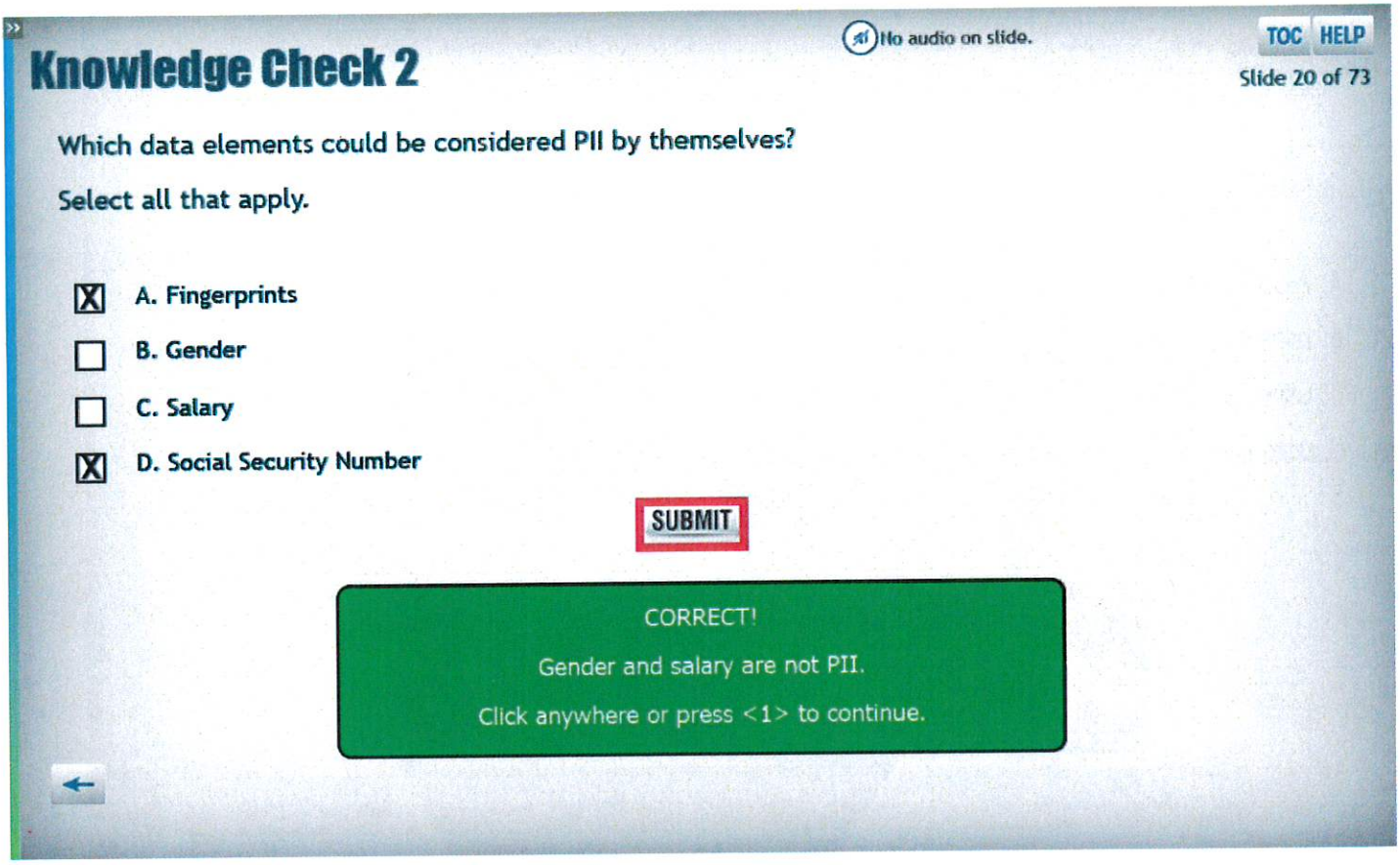
always remember to contact the Privacy Office for guidance before disclosing another individual's information.

Slide 21 - Knowledge Check 1



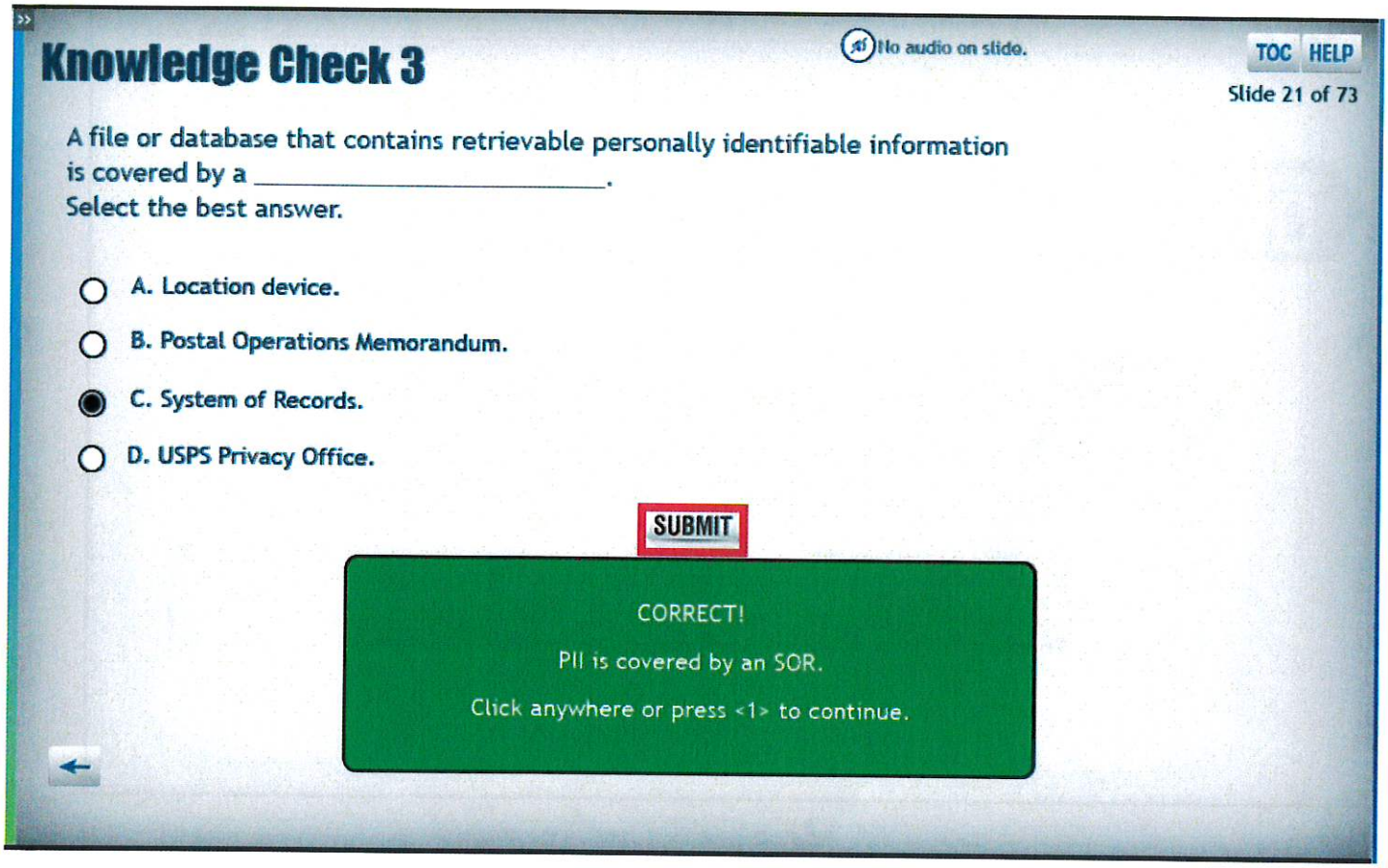
Slide notes

Slide 22 - Knowledge Check 2



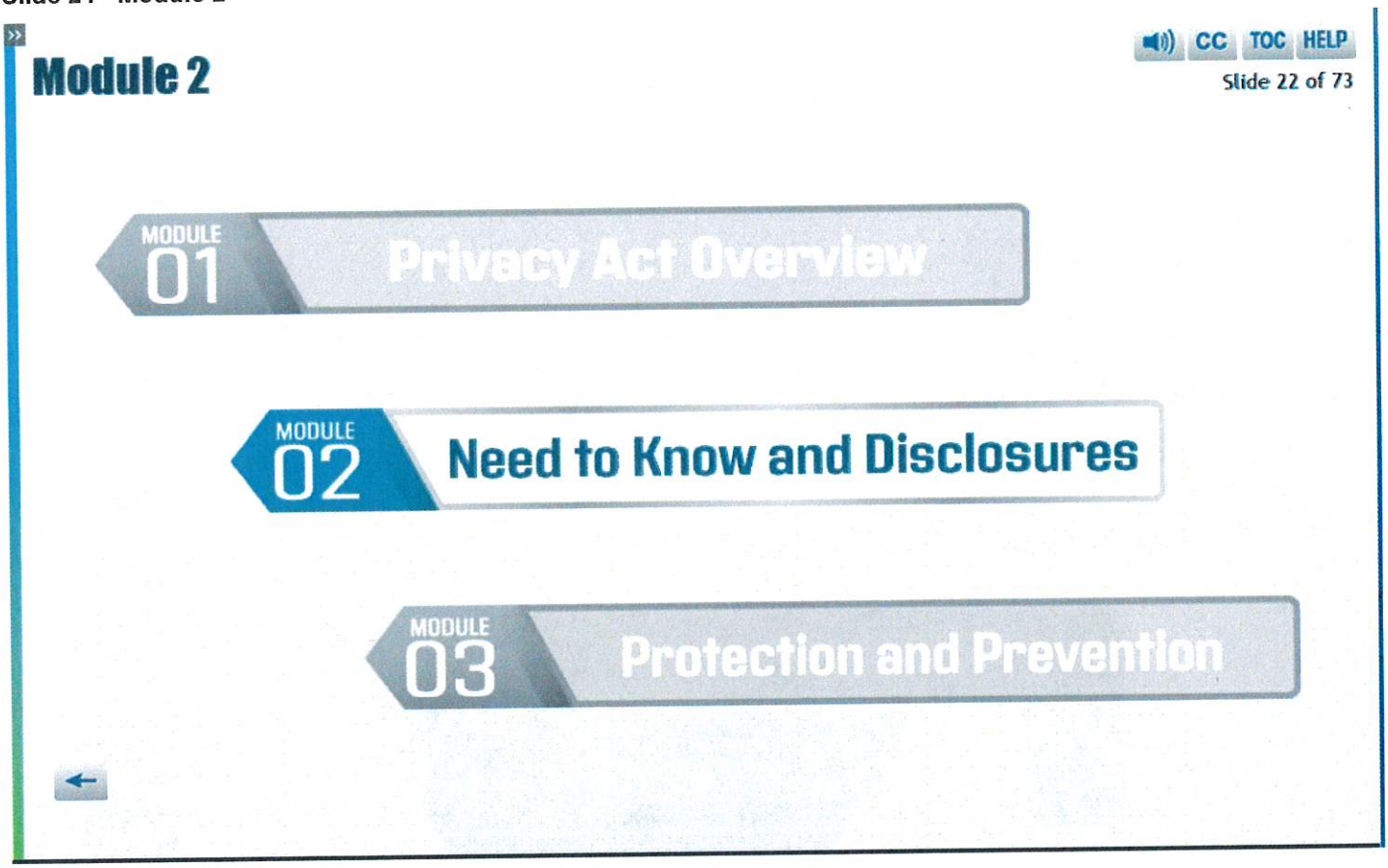
Slide notes

Slide 23 - Knowledge Check 3



Slide notes

Slide 24 - Module 2

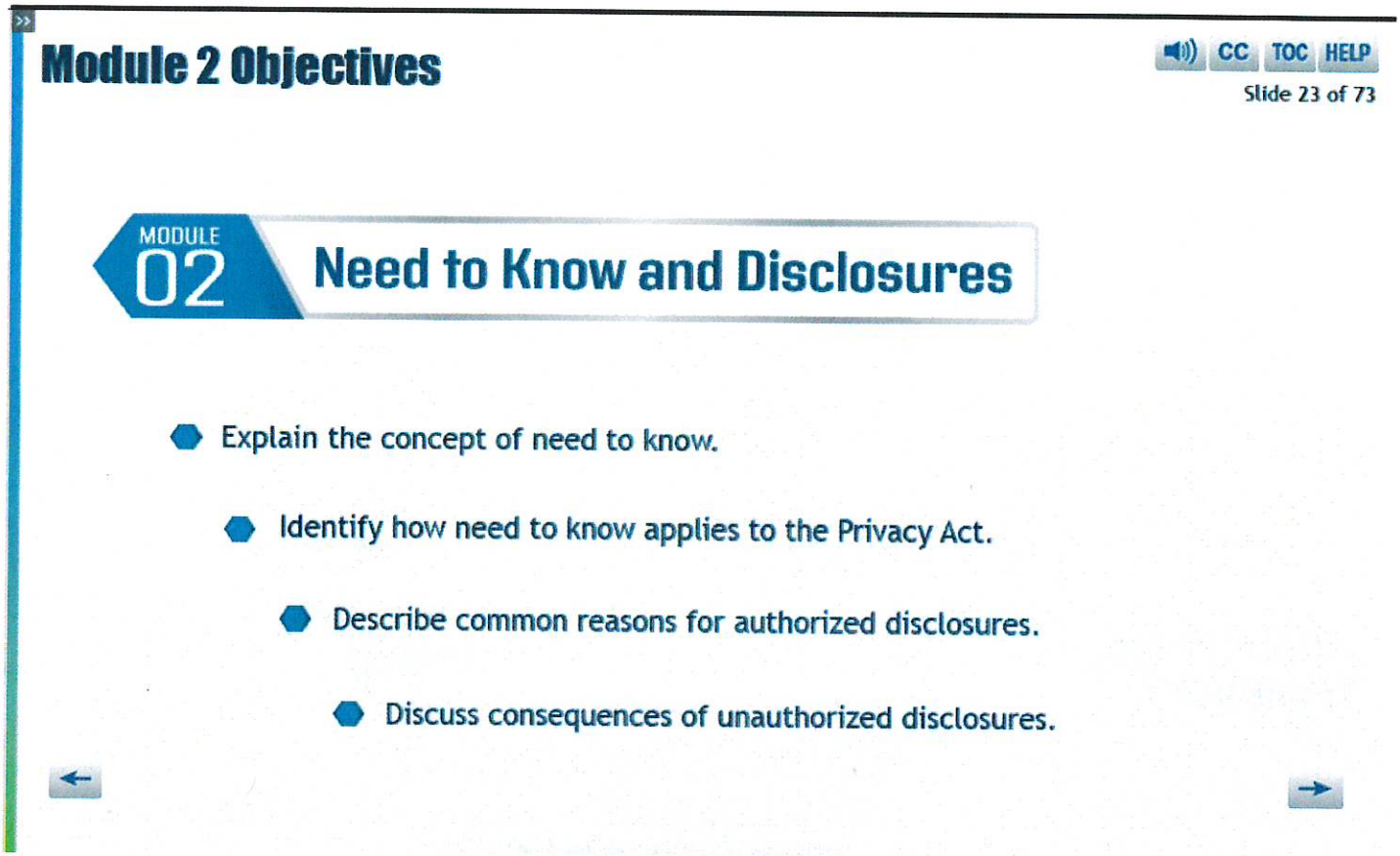


Slide notes

Welcome to Module 2, Need to Know and Disclosures. In this module, we'll go further in depth on the topics of need to know and disclosure.

To begin, click the Module 2 tile.

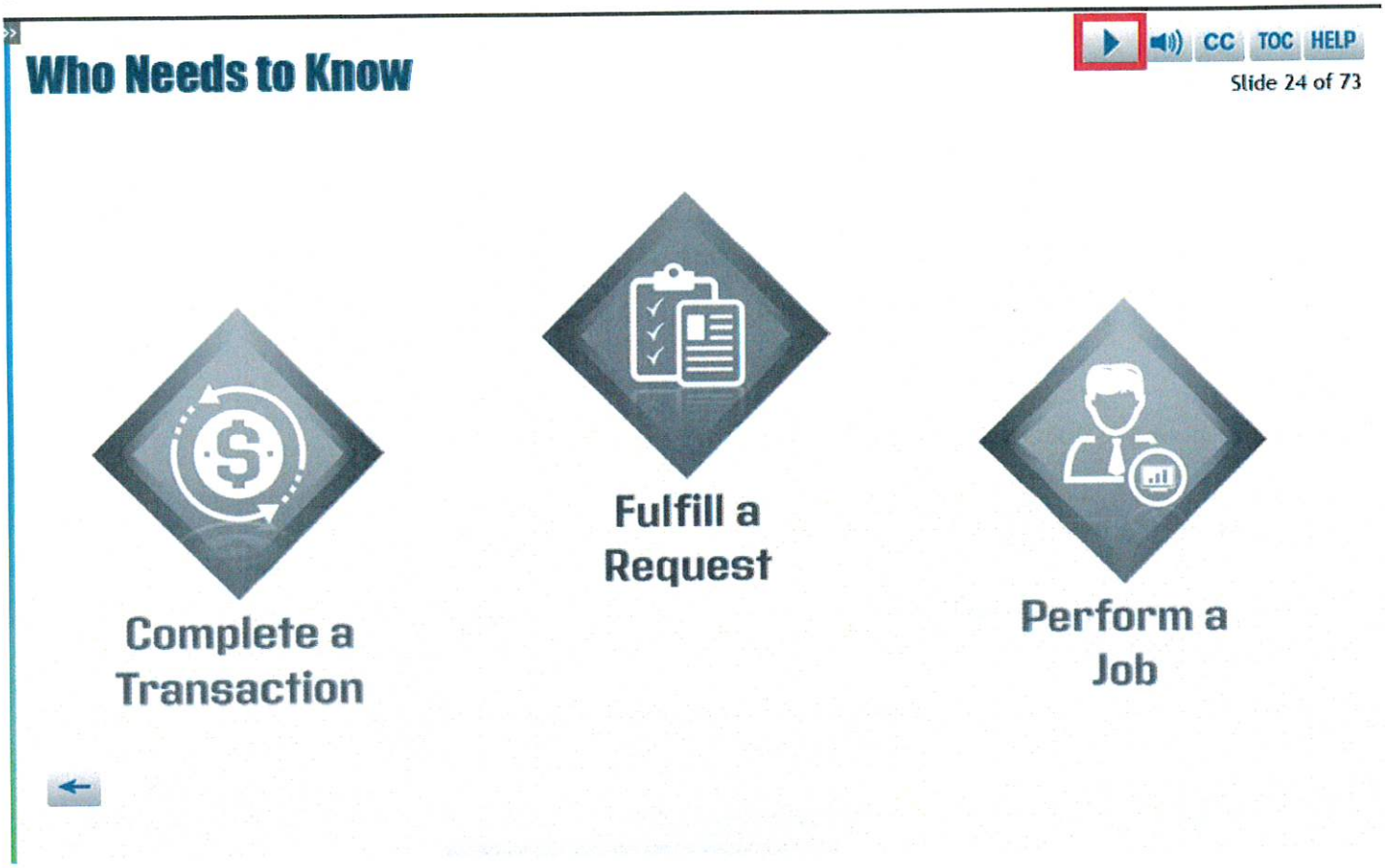
Slide 25 - Module 2 Objectives



Slide notes

By the end of this module, you should be able to explain the concept of need to know and identify how it applies to the Privacy Act, describe common reasons for authorized disclosures, and discuss consequences of unauthorized disclosures.

Slide 26 - Who Needs to Know



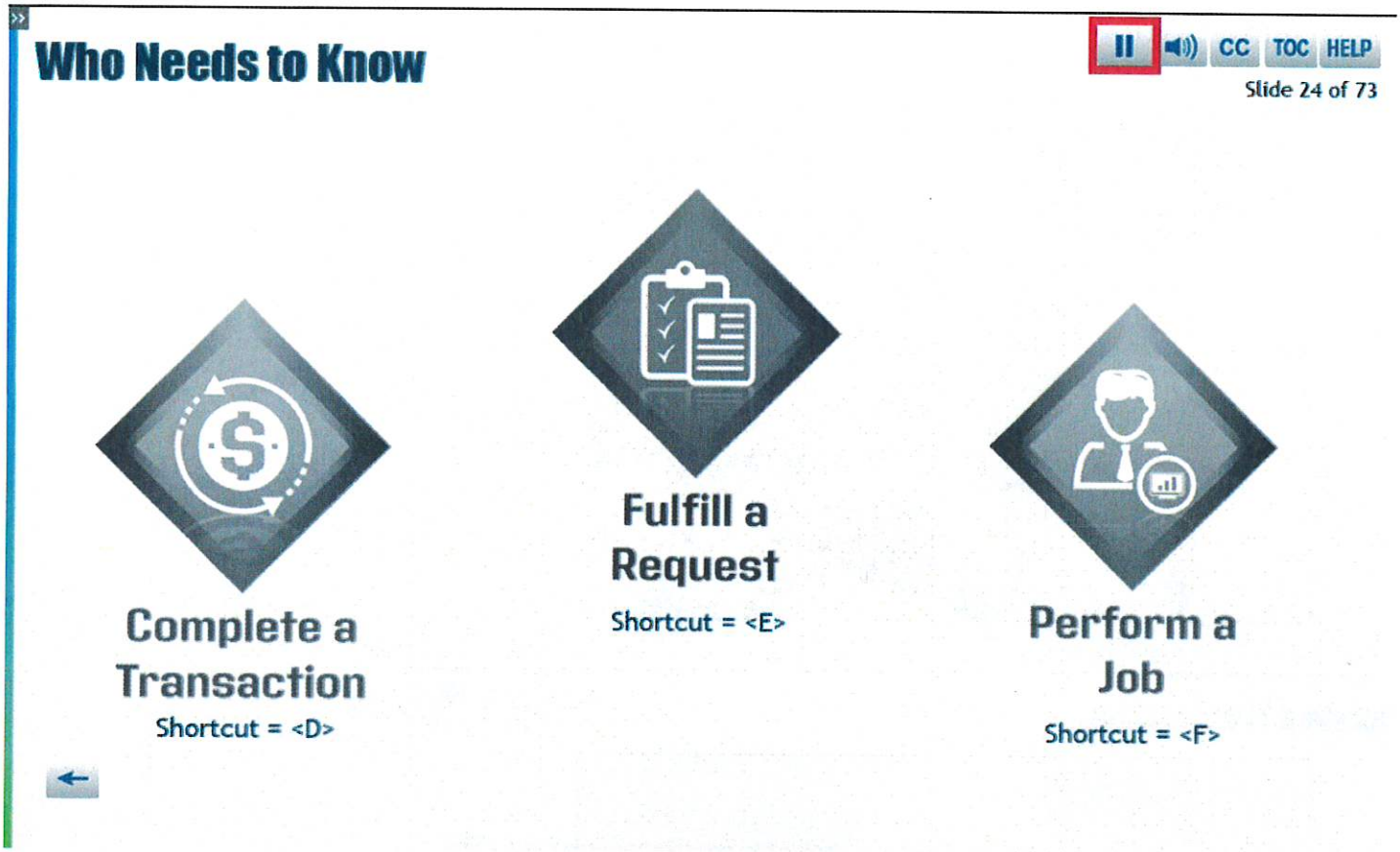
Slide notes

In the context of USPS, need to know largely pertains to internal employees and contractors

who need other individuals' personal information to complete a transaction, fulfill a request, or perform their job.

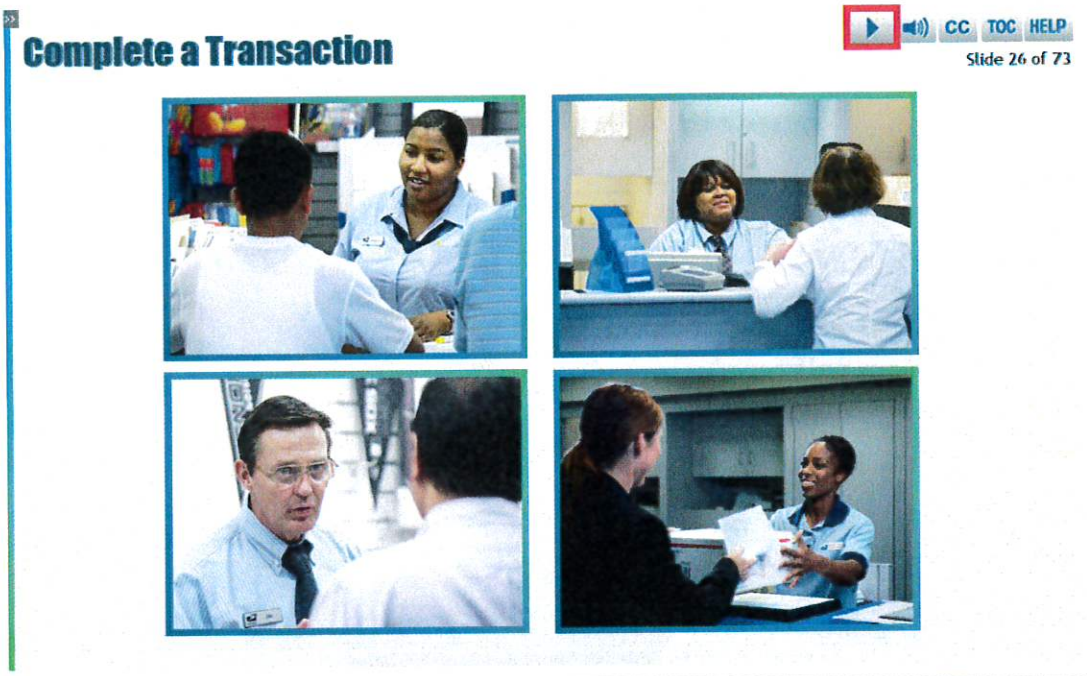
To review examples, click each image.

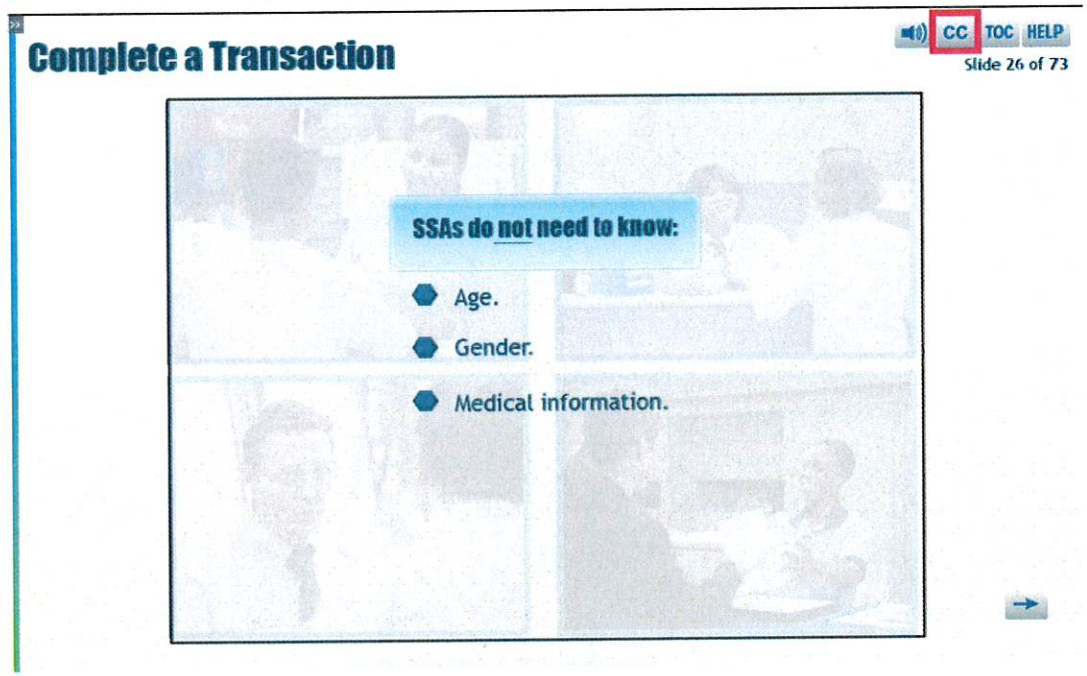
Slide 27 - NOT IN TOC



Slide notes

Slide 28 - Complete a Transaction



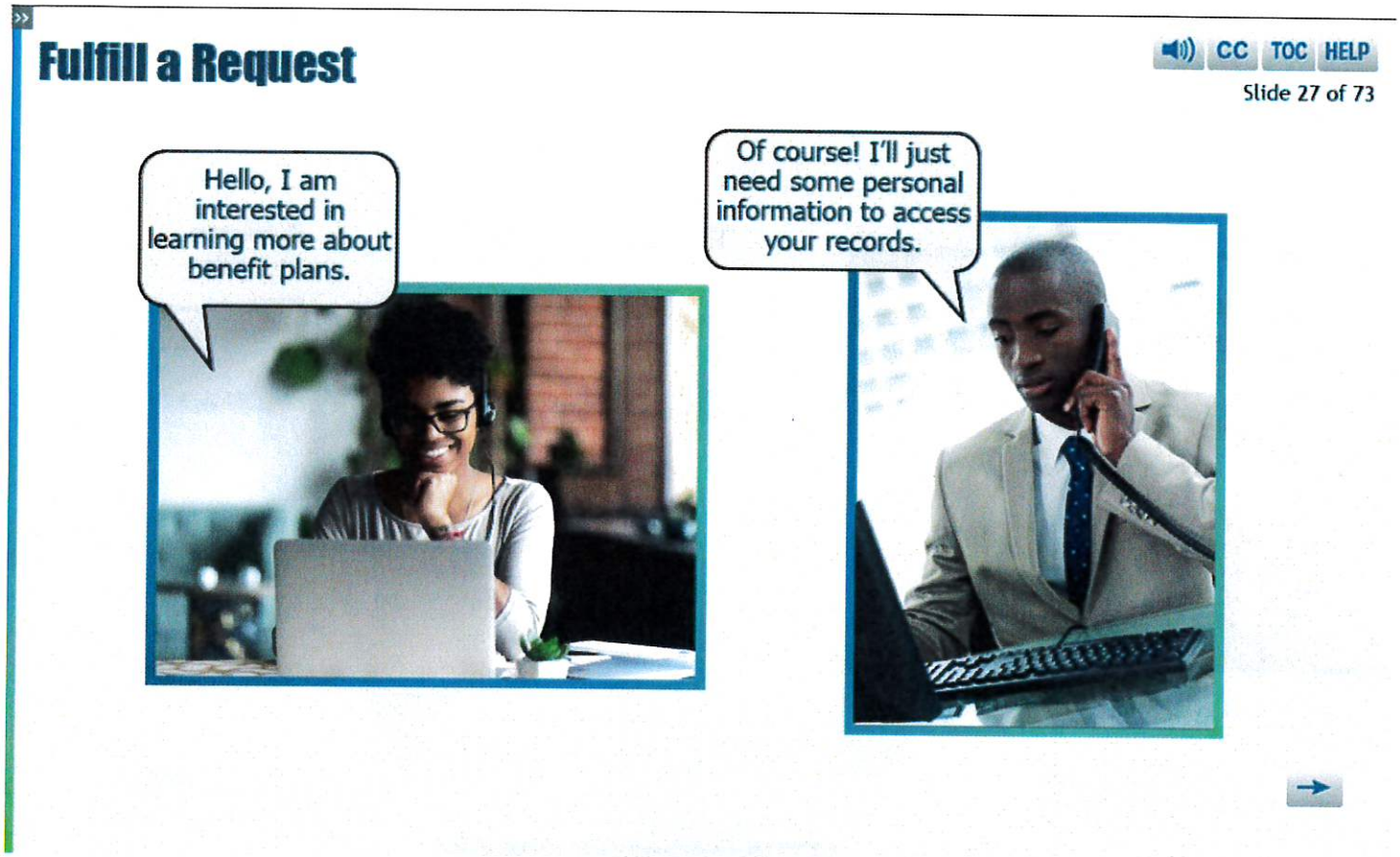


Slide notes

Sales and Services Associates (SSAs) have a need to know customers' full names, addresses, phone numbers, and email addresses in order to complete retail transactions.

SSAs do not have a need to know information such as age, gender, or medical information.

Slide 29 - Fulfill a Request

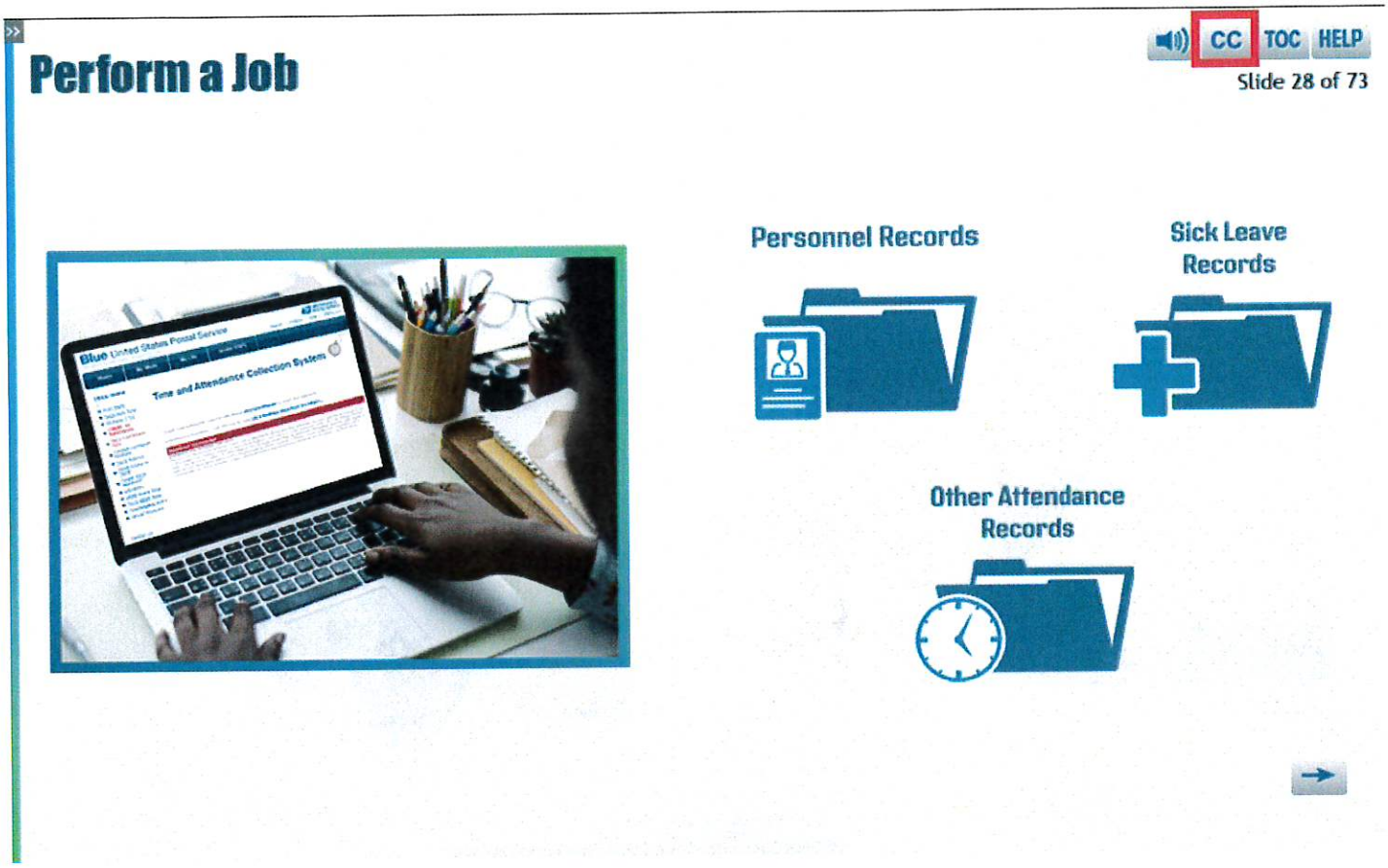


Slide notes

Should you need to call Human Resources, or HR, to inquire about benefit plans,

the HR representative would need to collect your PII so they can fulfill your request.

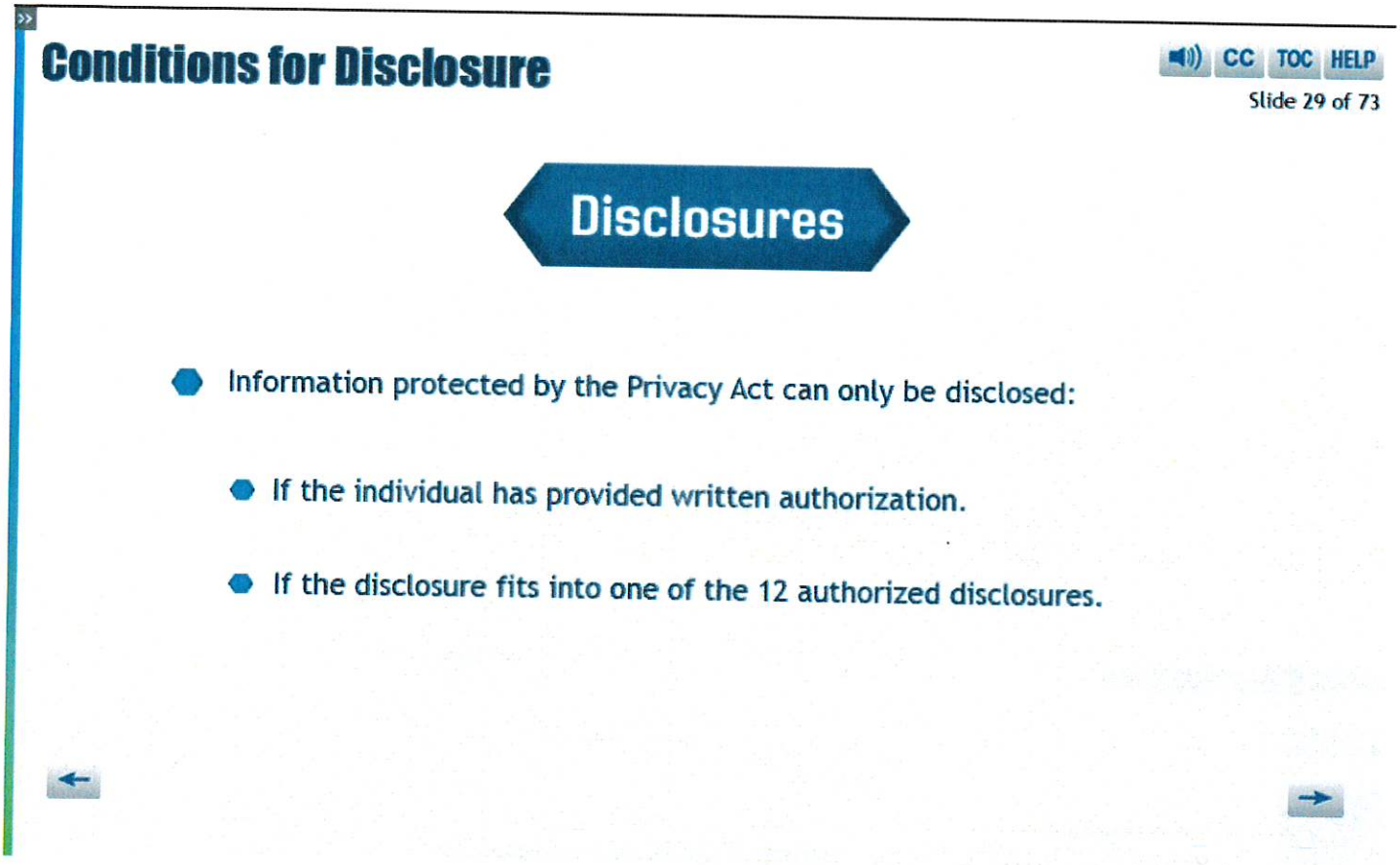
Slide 30 - Perform a Job



Slide notes

A person entering time and attendance has a need to know other employees' identification numbers, annual and sick leave balances, and what type of leave is being used.

Slide 31 - Conditions for Disclosure



Slide notes

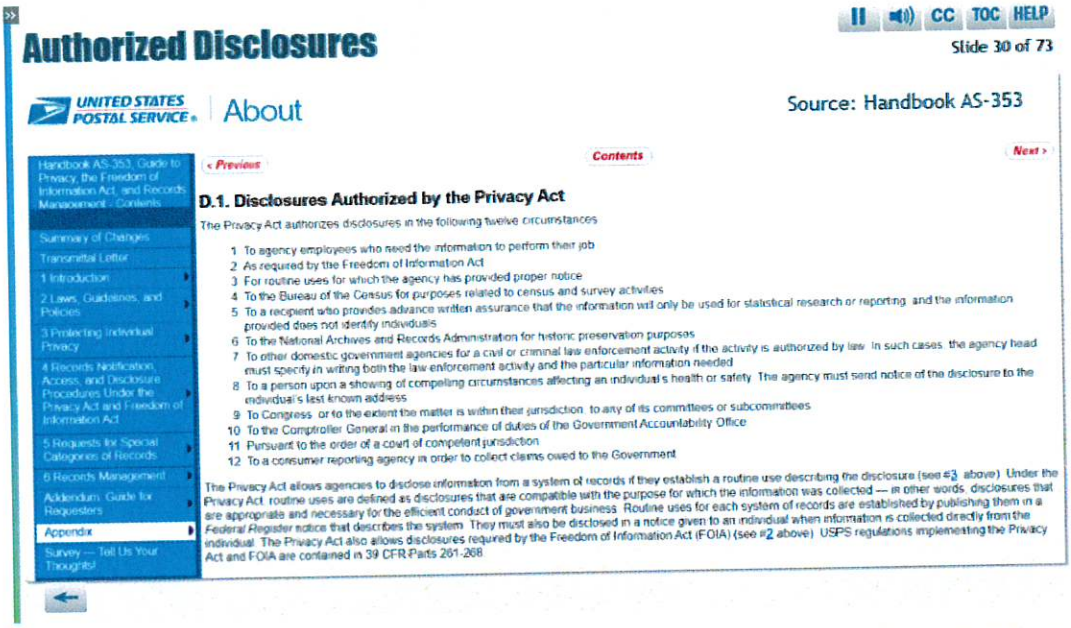
In Module 1, you learned the basic definition of a disclosure, but not specific examples of each.

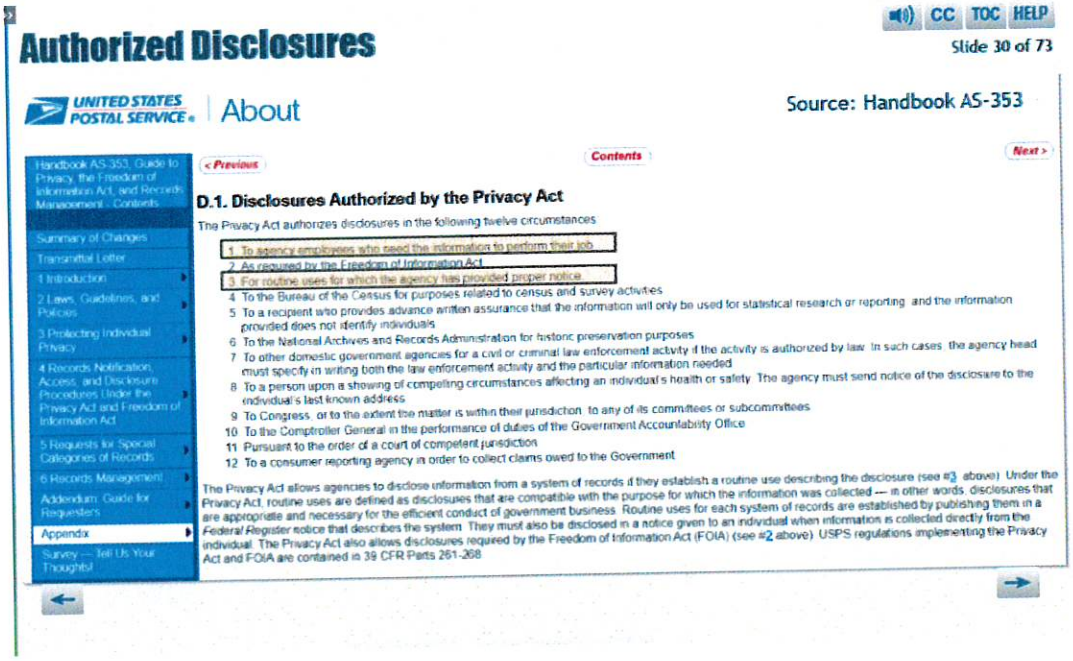
Information protected by the Privacy Act can only be disclosed under two conditions:

if the individual has provided written authorization or if the disclosure fits into one of the 12 authorized disclosures under the Privacy Act.

Let's look at those.

Slide 32 - Authorized Disclosures





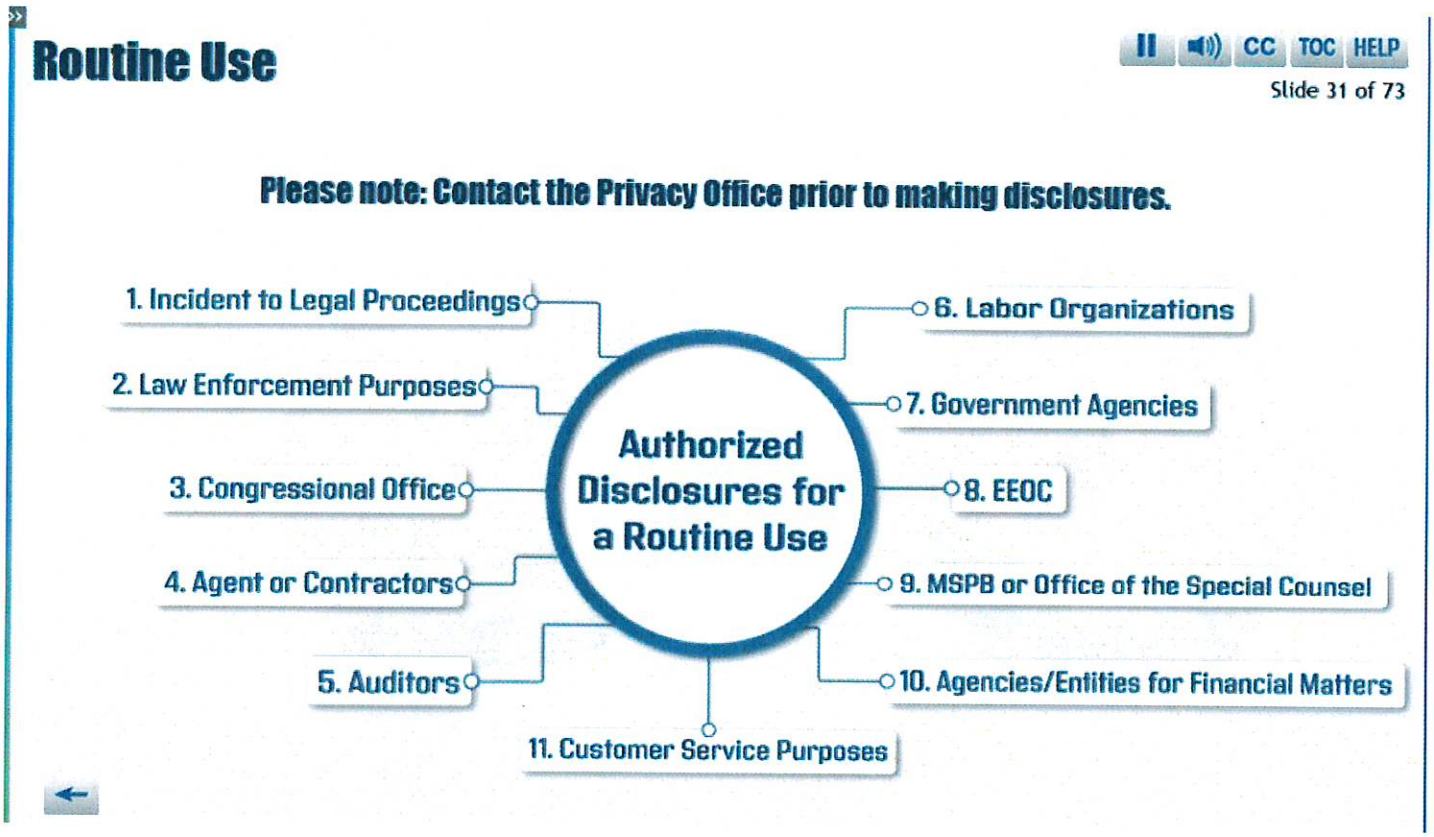
Slide notes

The Privacy Act authorizes disclosures under twelve circumstances.

Typically, the two types of authorized disclosures that will apply to you in the workplace

are the need to know to perform official job duties or under a USPS routine use.

Slide 33 - Routine Use



Slide notes

A routine use refers to authorized disclosures of information for recurring situations.

One example of a routine use is to provide the contractors who maintain the Informed Delivery platform with PII of USPS customers.

It is important to note, you must seek guidance from the Privacy Office to identify which records can be disclosed via a routine use.

Slide 34 - Common Scenarios

Common Scenarios

Slide notes

Now, let's review two workplace scenarios involving the Privacy Act.

To learn more, click each image.

Slide 35 - NOT IN TOC

Common Scenarios

Shortcut = <D>

Shortcut = <E>

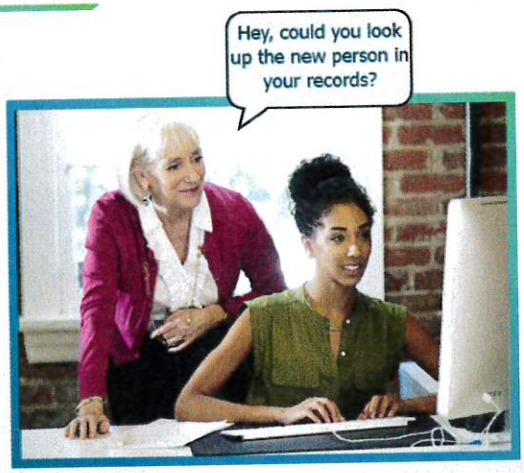
Slide notes

Slide 36 - Maya

Maya

CC TOC HELP

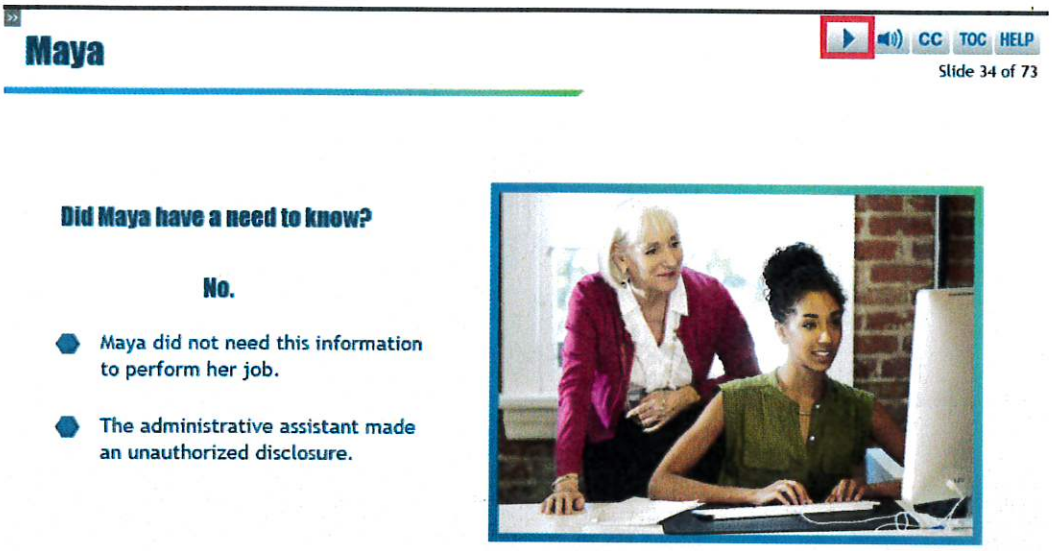
Slide 34 of 73

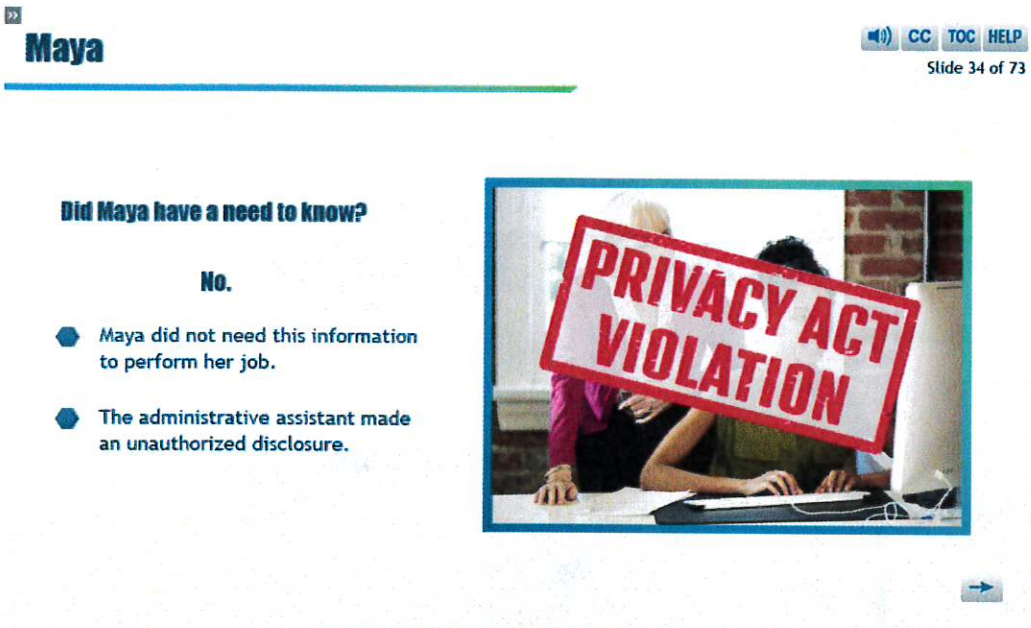


Maya

CC TOC HELP

Slide 34 of 73





Slide notes

Maya is curious about a new employee, so she asks her friend, an administrative assistant, to look at their personnel record.

Her friend doesn't see any harm and provides Maya with a name, home address, and personal cell phone number.

Do you think Maya had a need to know?

No. Maya did not need to know this information to perform her job,

and the administrative assistant made an unauthorized disclosure.

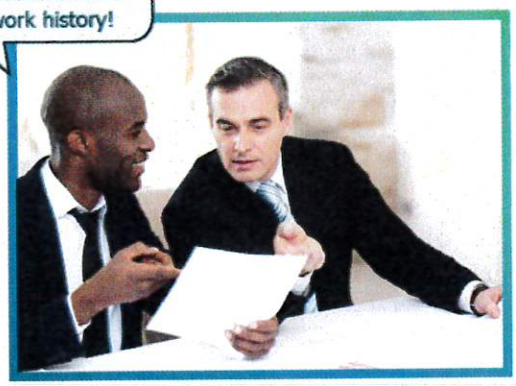
Slide 37 – Philip

Philip

CC TOC HELP

Slide 35 of 73

I found this resume on the printer. Check out their work history!



Philip

CC TOC HELP

Slide 35 of 73

Do you think this is an example of a routine use?

No.

- Neither person had a need to know this information to perform a job.
- The person who printed the resumes has violated the Privacy act by not safeguarding the PII.

Philip

CC TOC HELP

Slide 35 of 73

Do you think this is an example of a routine use?

No.

- Neither person had a need to know this information to perform a job.
- The person who printed the resumes has violated the Privacy act by not safeguarding the PII.

Slide notes

Philip finds a stack of resumes on the printer, so he skims through a couple of them,

then he shares one of the resumes with a coworker.

Do you think this is an example of a routine use?

No. Neither of these gentlemen had a need to know this information,

and whomever printed the resumes has violated the Privacy Act by not safeguarding the PII.

Slide 38 - Third-Party Disclosures

Third-Party Dislosures

CC TOC HELP
Slide 36 of 73

- Third-party disclosures:
  - Made to outside agencies, individuals, or businesses who request information covered by a USPS SOR
- Examples:
  - Former employee authorizes disclosure of their own information when pursuing a new job
  - During divorce or civil proceeding

Slide notes

Third-party disclosures are made to outside agencies, individuals,

or businesses who request information covered by a USPS Privacy Act System of Records.

Two common scenarios of this are when a former employee authorizes the disclosure of their own information for a job search

or during a divorce or civil proceeding.

Slide 39 - Special Categories of Records

Slide notes

Certain categories of records within an SOR may be requested frequently and involve special processing.

These include requests from Congressional committees, courts or attorneys, collective bargaining units,

the news media, or for employee surveys.

Again, seek direction and guidance from the Privacy Office prior to disclosing records.

Slide 40 - Unauthorized Disclosures

Slide notes

An unauthorized disclosure is an improper transfer, sharing, or exposure of information pertaining to PII of an individual.

This can happen via email, paper documents, phone calls, social media, or conversations.

Let's review more scenarios involving unauthorized disclosures. To learn more, click each icon.

Slide 41 - NOT IN TOC

Unauthorized Disclosures

CC TOC HELP

Slide 39 of 73

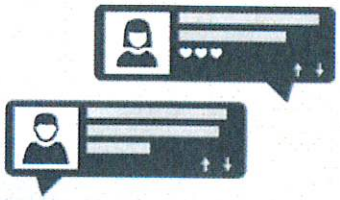
Unauthorized disclosure: An improper transfer, sharing, or exposure of PII

Email

Shortcut = <D>

In-Person Discussion

Shortcut = <E>



Posting Online

Shortcut = <F>

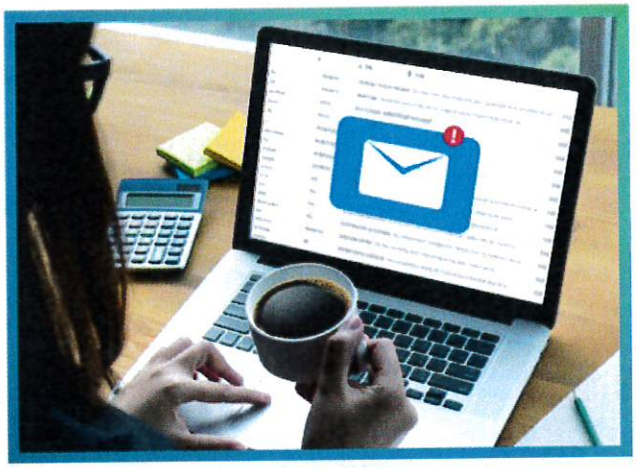
Slide notes

Slide 42 – Email

Email

CC TOC HELP

Slide 40 of 73



Prior to a Zoom meeting, a manager forwards a complete list of department sick leave information to all three of their direct reports and then reviews the information on the group call.

Email

CC TOC HELP

Slide 40 of 73

Prior to a Zoom meeting, a manager forwards a complete list of department sick leave information to all three of their direct reports and then reviews the information on the group call.

Email

CC TOC HELP
Slide 40 of 73

Prior to a Zoom meeting, a manager forwards a complete list of department sick leave information to all three of their direct reports and then reviews the information on the group call.

Unauthorized disclosures:

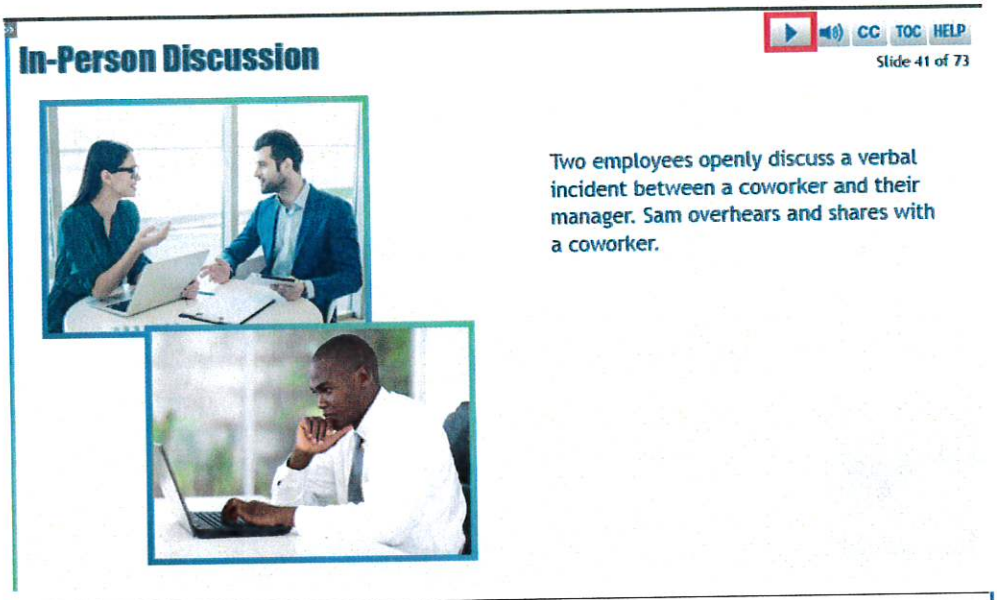
- The manager did not separate the PII into three manager specific reports.

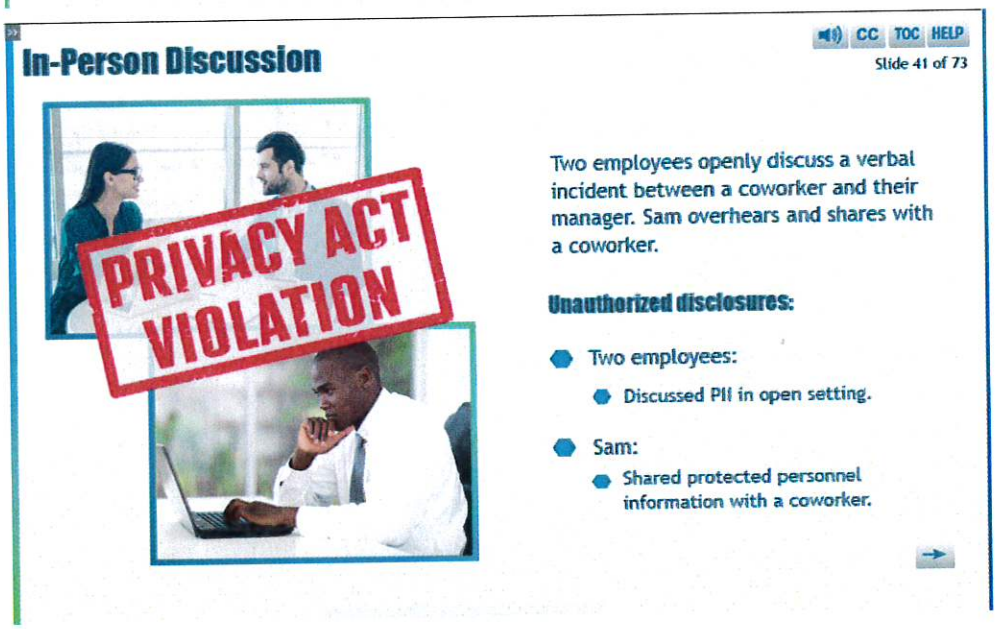
Slide notes

Prior to a Zoom meeting, a manager receives an email containing PII for all employees in their department and forwards the complete list to their three direct reports.

This means the manager made three unauthorized disclosures by not separating the personal information into three manager specific reports.

Slide 43 - In-Person Discussion





Slide notes

Two employees, sitting in an open meeting space, are discussing disciplinary actions of an employee named Tru.

Sam, working at a desk nearby, overhears the conversation and is able to identify the employee by name and department.

Sam then shares what he heard with another employee.

Since the contents of personnel files are protected under an SOR, two unauthorized disclosures were made.

The two employees made an unauthorized disclosure when they discussed PII in an open setting,

and Sam made an unauthorized disclosure to his friend.

Slide 44 - Social Media

Social Media

CC TOC HELP

Slide 42 of 73

Ahmad learns a customer has been injured, so he obtains the new address from the Change of Address system.

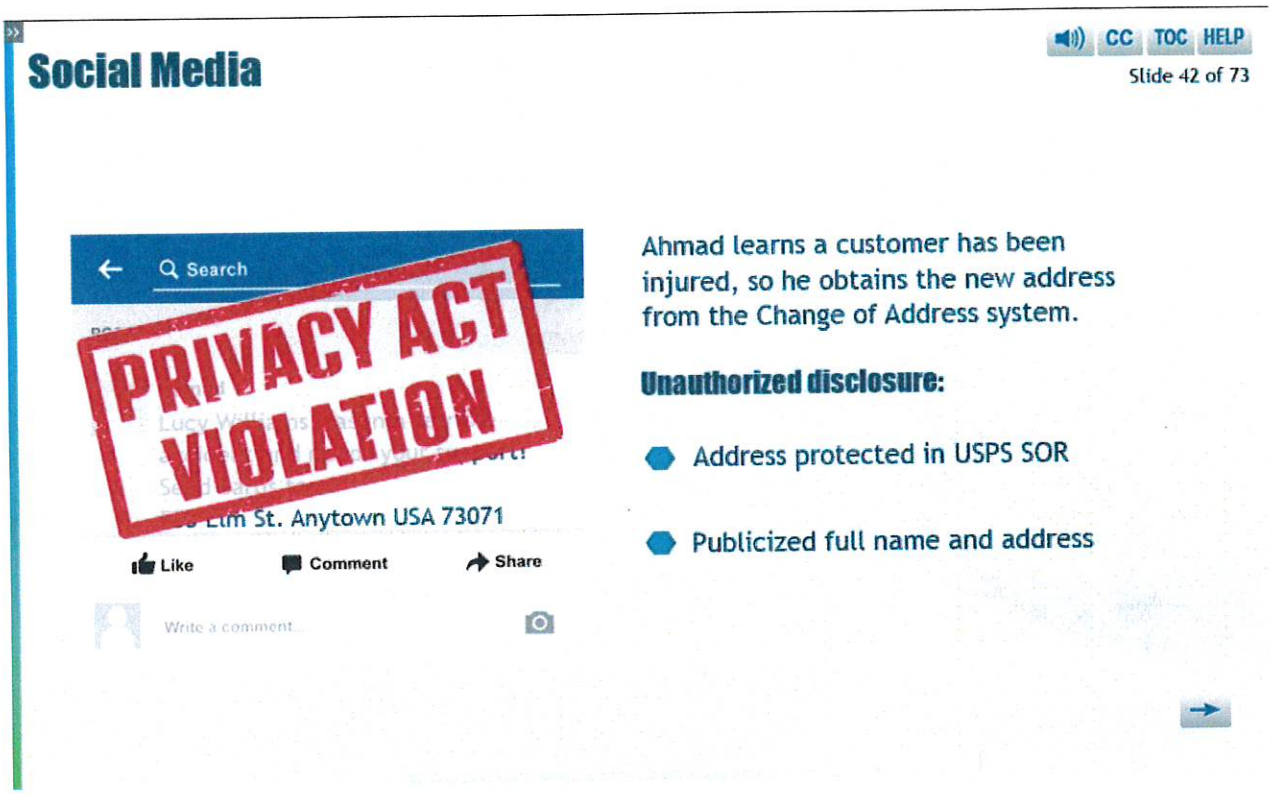
Social Media

CC TOC HELP

Slide 42 of 73

Ahmad learns a customer has been injured, so he obtains the new address from the Change of Address system.

Unauthorized disclosure:



Slide notes

Ahmad, a letter carrier, learns that a customer on his previous route has been injured in an auto accident.

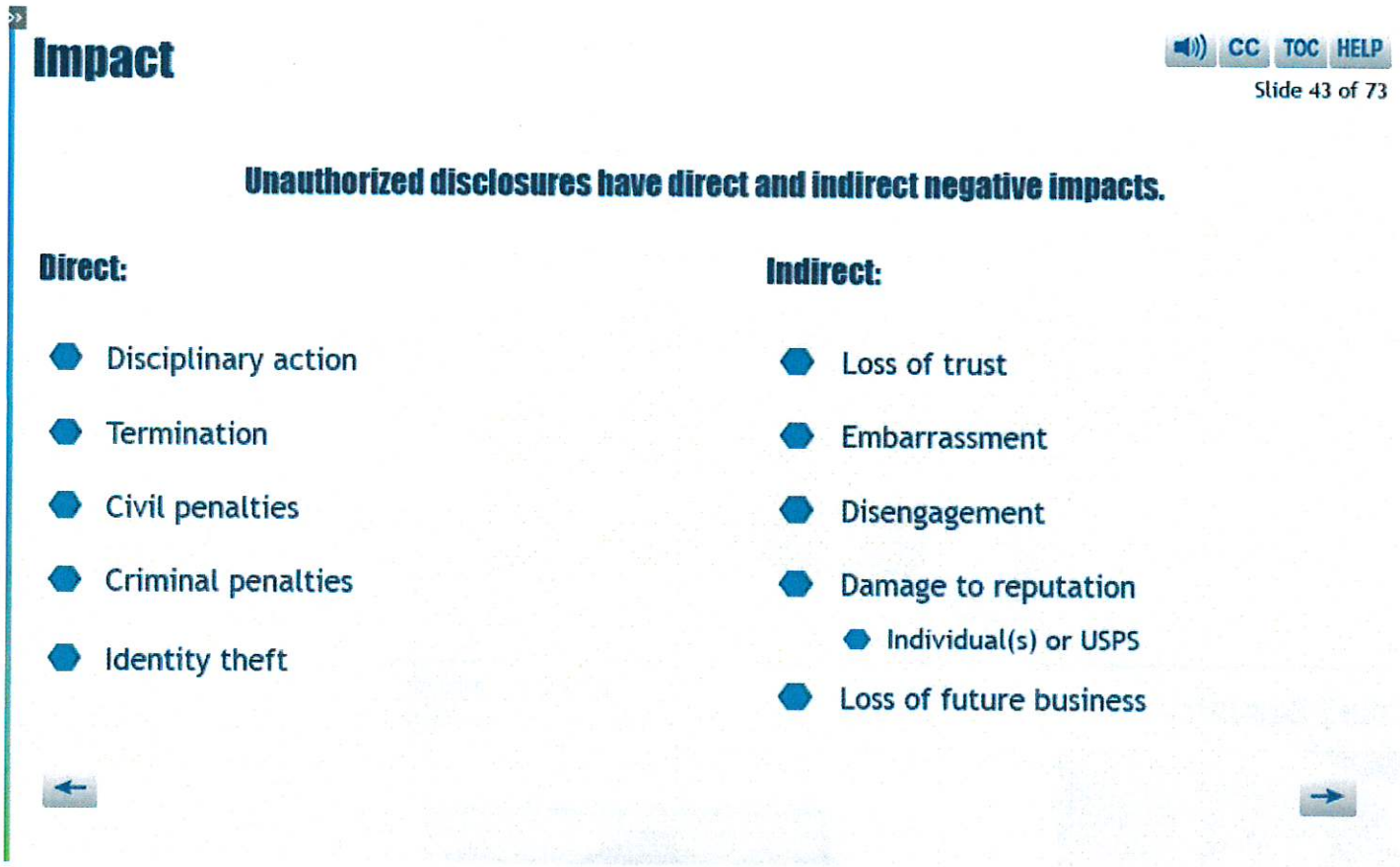
He decides it would be a good idea to have people send them cards and letters of support,

but remembers they recently moved, so he obtains the new address from the Change of Address system,

which is covered under an SOR, and publicizes the customer's full name and address on social media.

Ahmad has violated the Privacy Act by making an unauthorized disclosure of PII.

Slide 45 - Impact



Slide notes

Unauthorized disclosures have direct and indirect negative impacts.

Direct consequences include, but are not limited to, disciplinary action, termination, civil penalties, criminal penalties, and even identity theft.

Less direct effects include a loss of trust, embarrassment, disengagement, damage to the reputation of individuals or USPS,

and possibly a loss of future business if the incident damages the USPS brand.

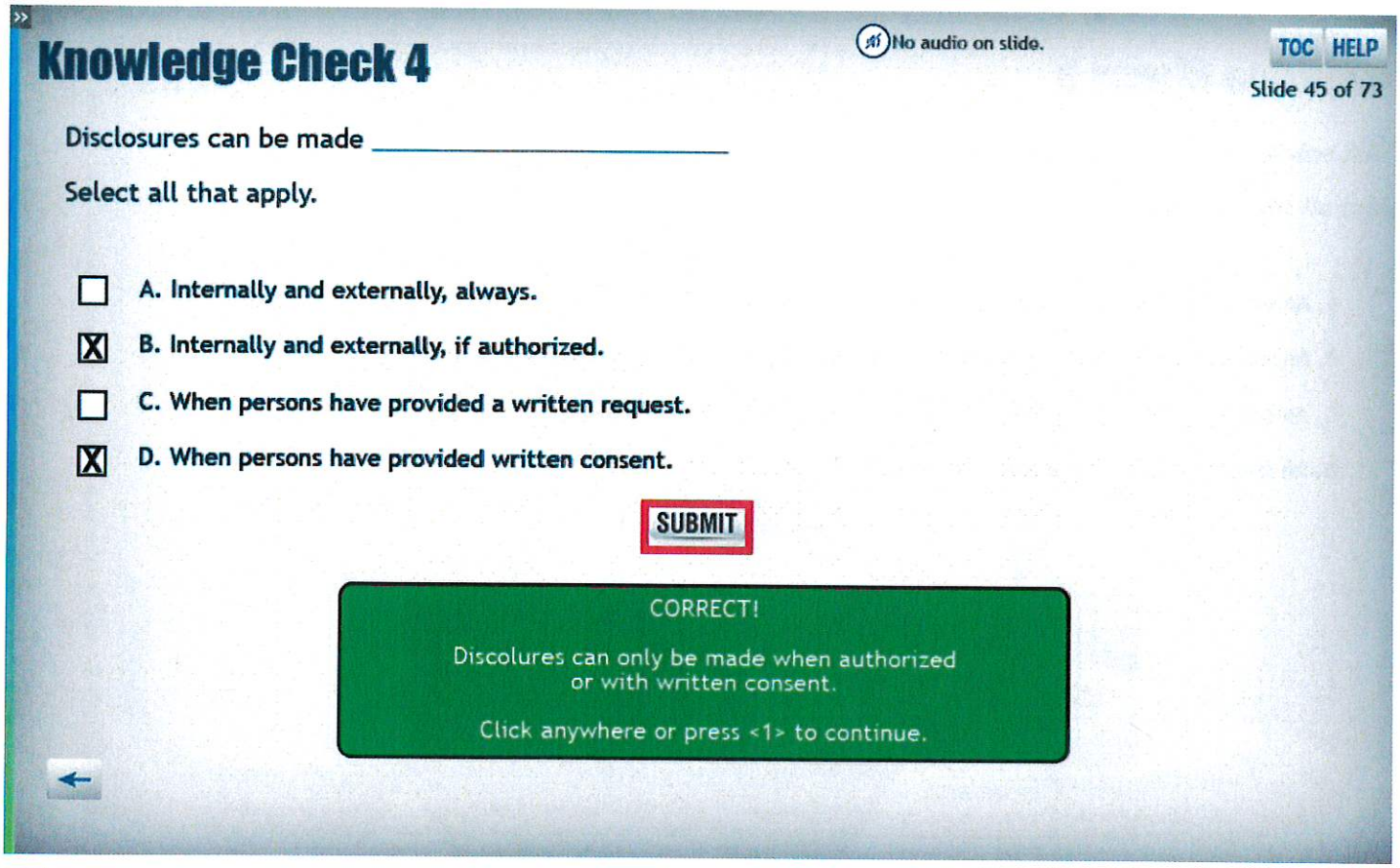
Slide 46 - Module 2 Summary

Slide notes

To review, personal information USPS collects must only be disclosed to persons who have a validated need to know or to those whom have submitted a written request for their own information.

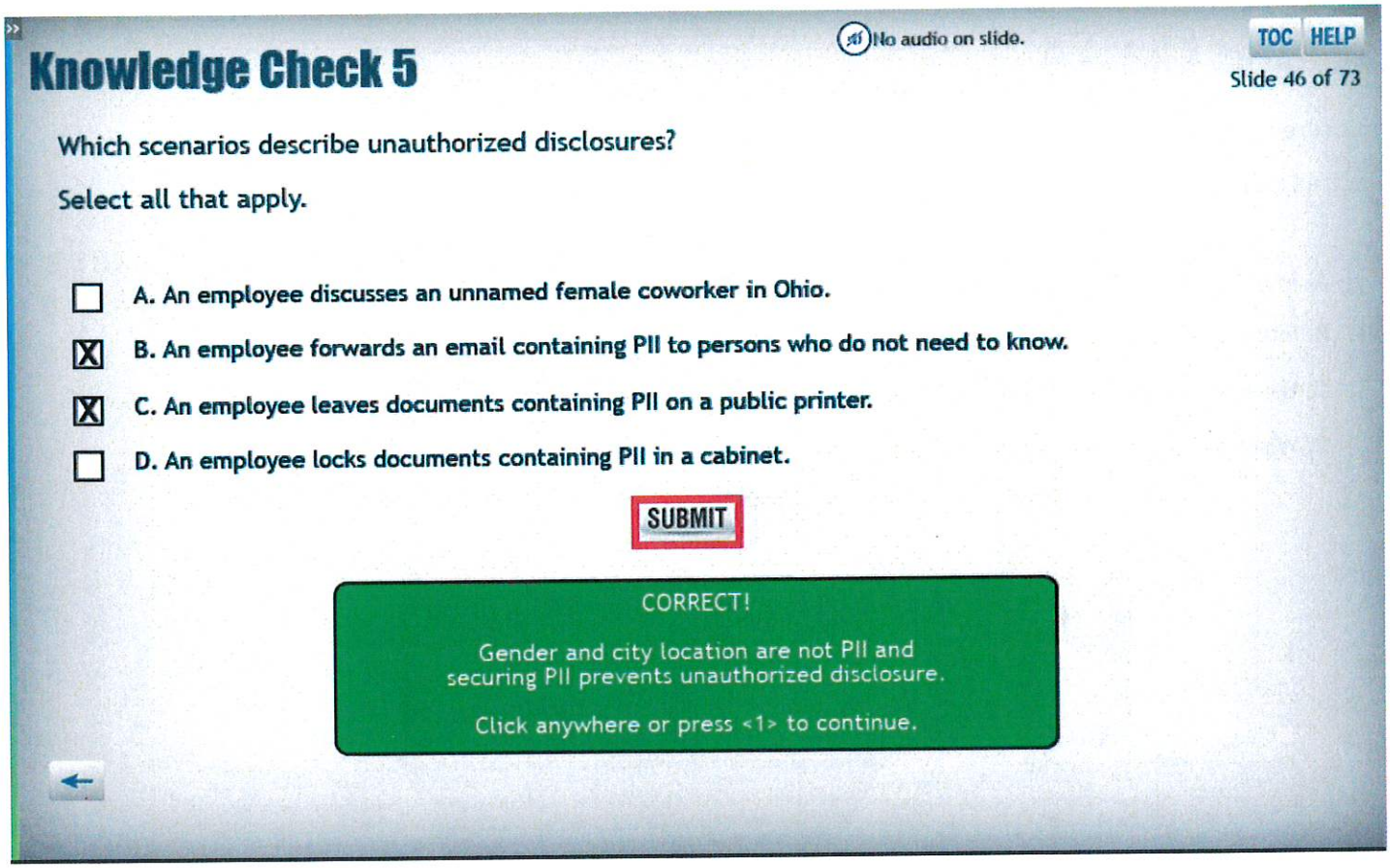
It is important to consider the very real impact of unauthorized disclosures, which could result in direct and indirect costs that negatively impact the individual and/or USPS.

Slide 47 - Knowledge Check 4



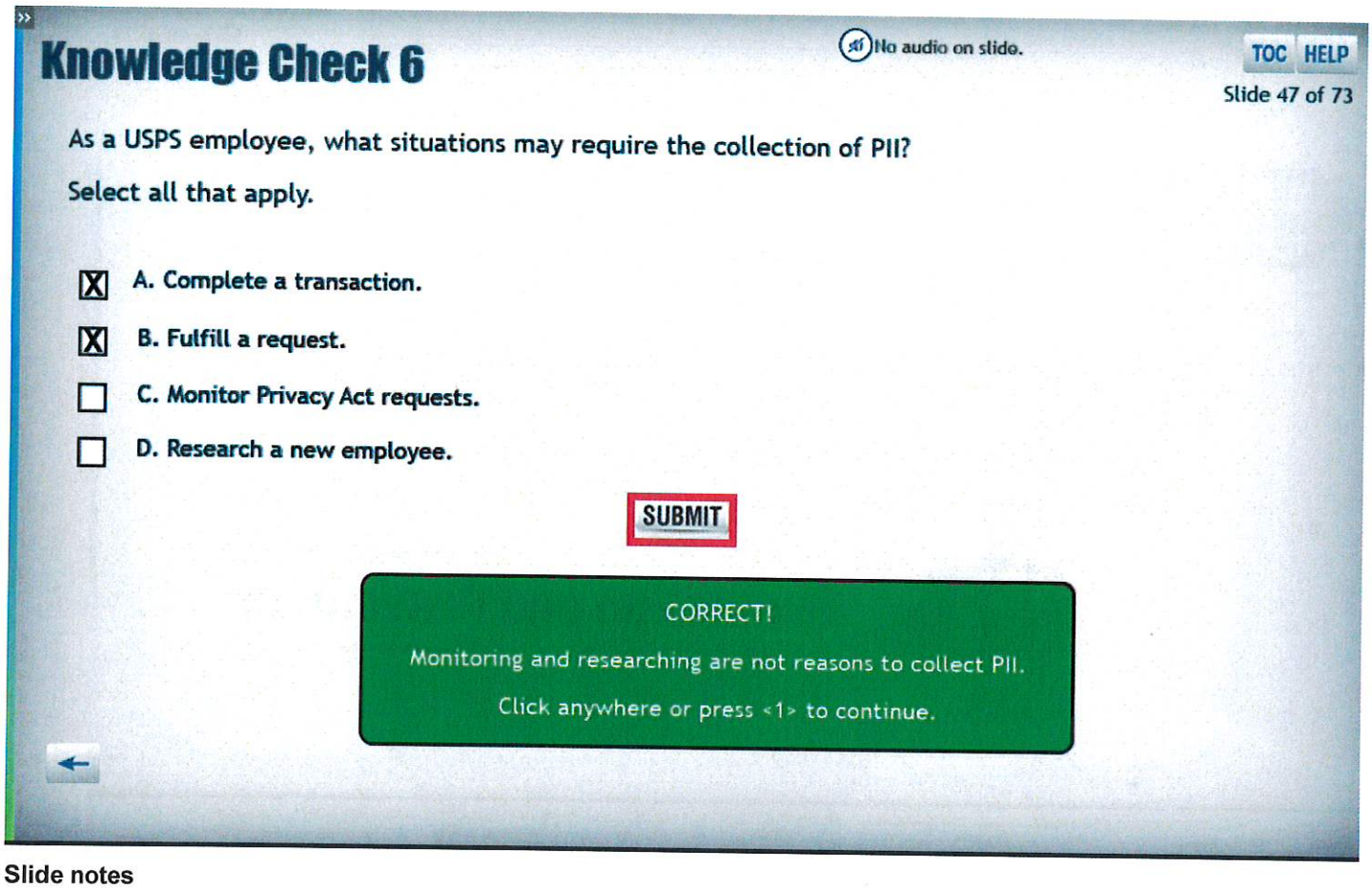
Slide notes

Slide 48 - Knowledge Check 5



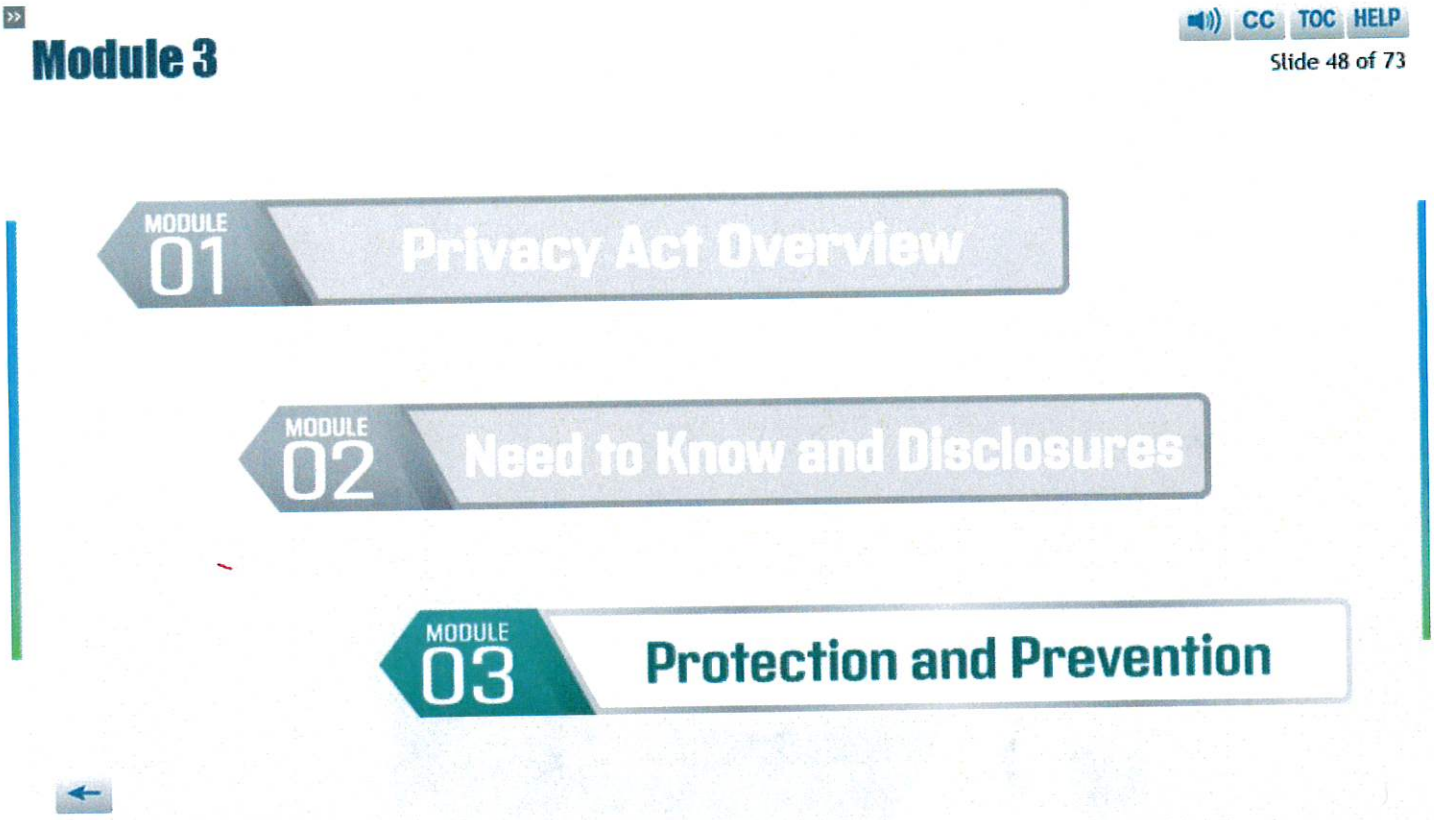
Slide notes

Slide 49 - Knowledge Check 6



Slide notes

Slide 50 - Module 3



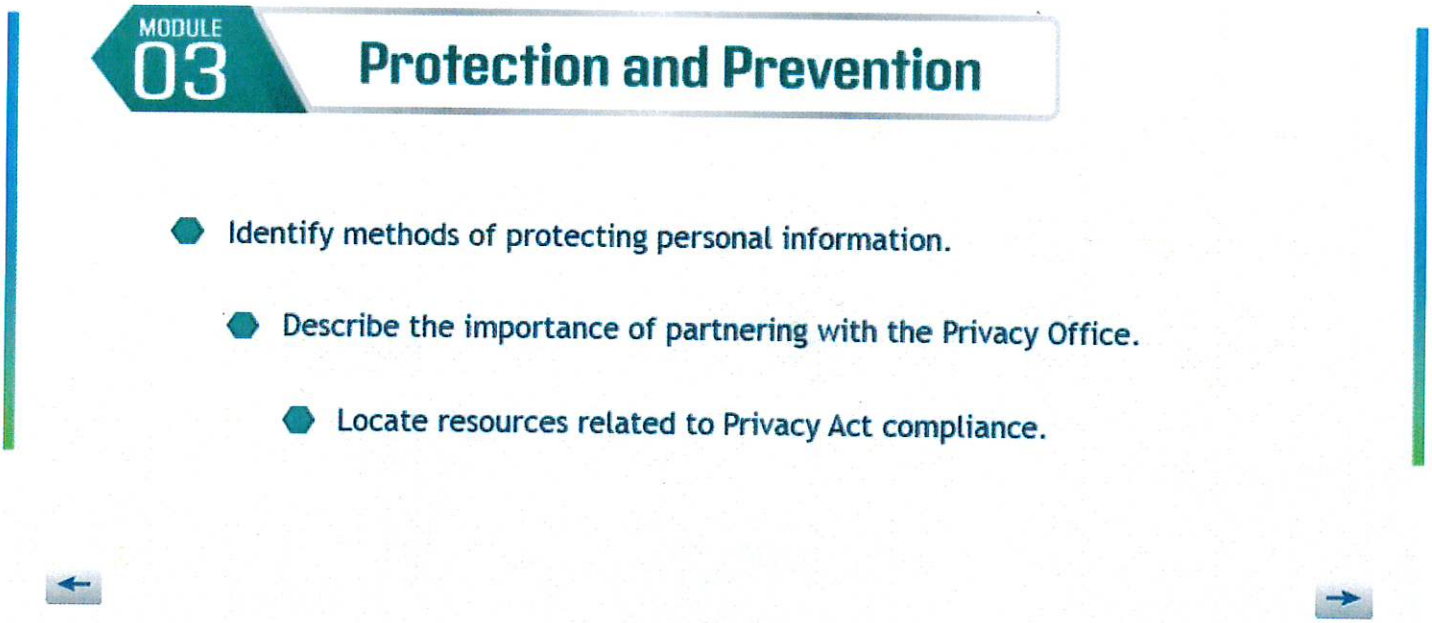
Slide notes

Welcome to Module 3, Protection and Prevention. In this module, we'll discuss how you can actively protect and secure PII against unauthorized disclosures and prevent costly delays by partnering with the Privacy Office for new projects.

To begin, click the Module 3 tile.

Slide 51 - Module 3 Objectives

Module 3 Objectives



Slide notes

By the end of this module, you should be able to identify methods of protecting personal information,

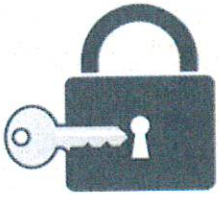
describe the importance of partnering with the Privacy Office, and locate resources related to Privacy Act compliance.

Slide 52 - Protecting PII

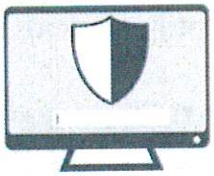
Protecting PII

Administrative

Physical



Technical



Slide notes

The Privacy Act requires USPS to use administrative, physical, and technical safeguards to protect personal information.

To learn more, click each icon.

Slide 53 - NOT IN TOC

Protecting PII

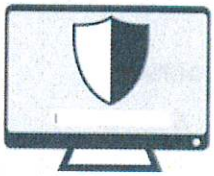
Administrative

Shortcut = <E>

Physical

Shortcut = <F>

Technical



Shortcut = <G>

Slide notes

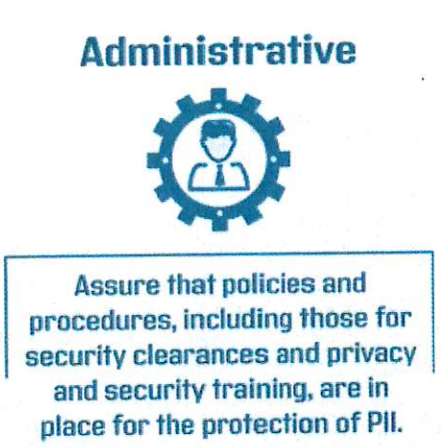
Slide 54 - Administrative

Administrative

CC TOC HELP
Slide 52 of 73

Administrative Protective Measures:

- Policies and procedures regarding security
- Security clearance levels
- Training courses



Slide notes

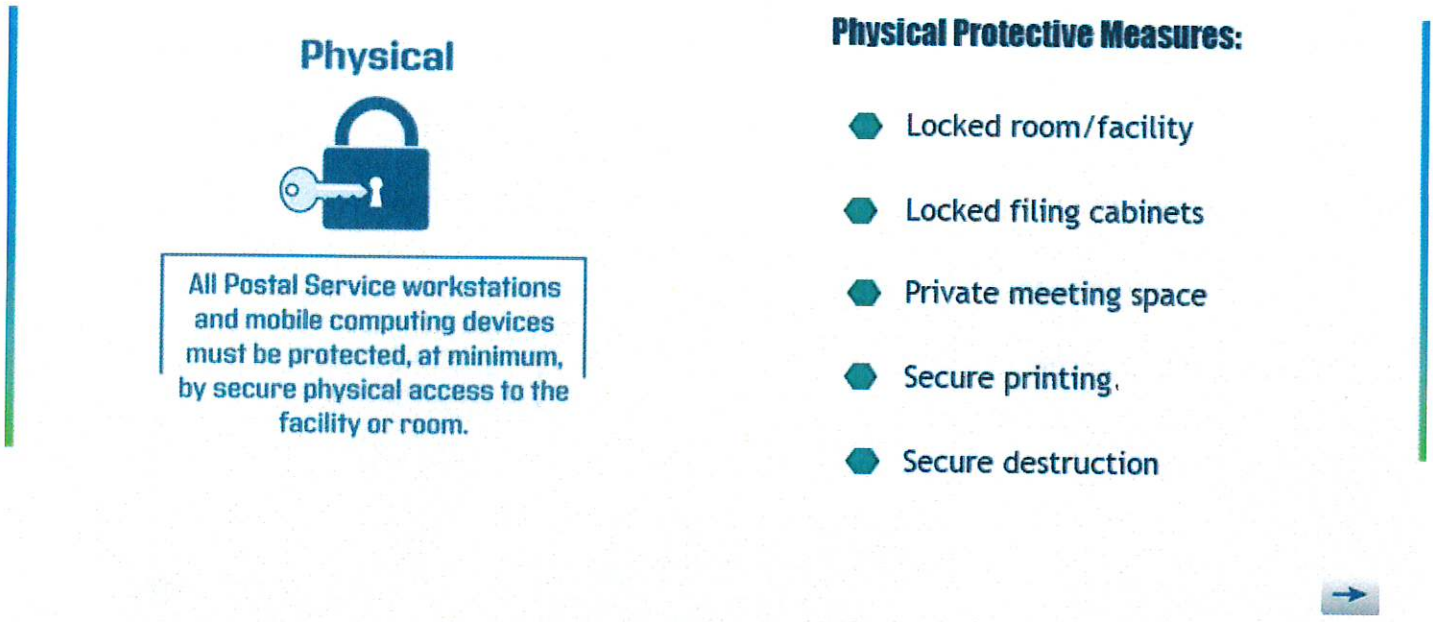
Protecting PII through administrative methods means having policies and procedures in place to secure records, issue different levels of security clearances, and regularly provide training courses, such as this one.

Slide 55 - Physical

Physical

CC TOC HELP

Slide 53 of 73



Slide notes

Physical protective measures include housing all USPS workstations in a locked room or facility, storing paper documents in locked cabinets, holding sensitive in-person or phone conversations in a private setting, and using both secure printing and secure destruction methods to safeguard PII from unintended viewing.

Slide 56 - Technical

Technical

Technical Protective Measures:

- Firewalls
- Access management programs
- Encryption - transmission and storage
- Logging off workstation

Technical

Have technical safeguards, such as firewalls, access management, transmission security, and data encryption.

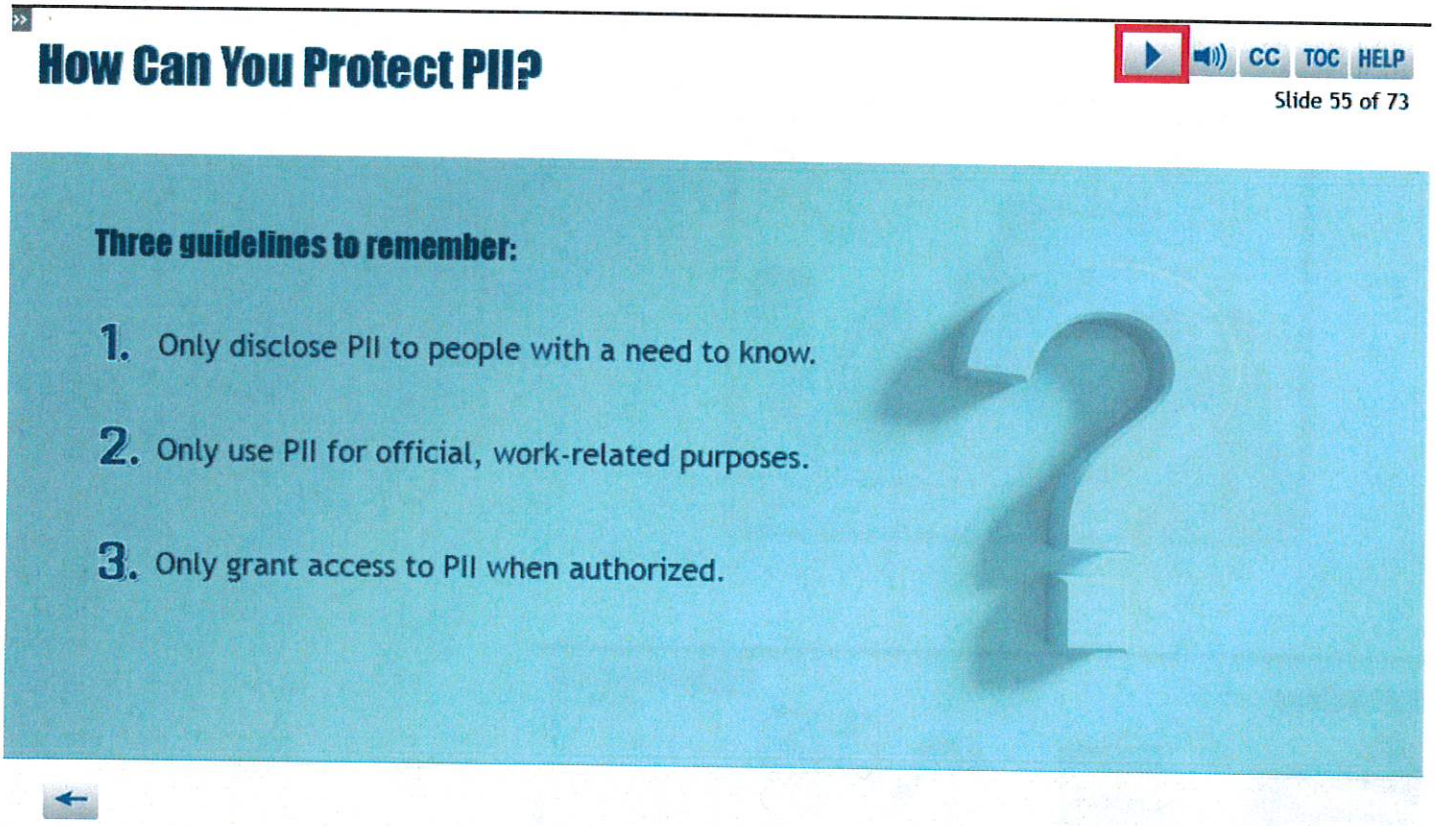
Slide notes

Technical safeguards include firewalls, access management programs,

and storage or transmission security, such as encryption.

Logging off your workstation is also a critical component of maintaining security.

Slide 57 - How Can You Protect PII?



Slide notes

So, how can you prevent the unauthorized access, collection, disclosure, or misuse of personal information? It's easy!

Just remember these three guidelines.

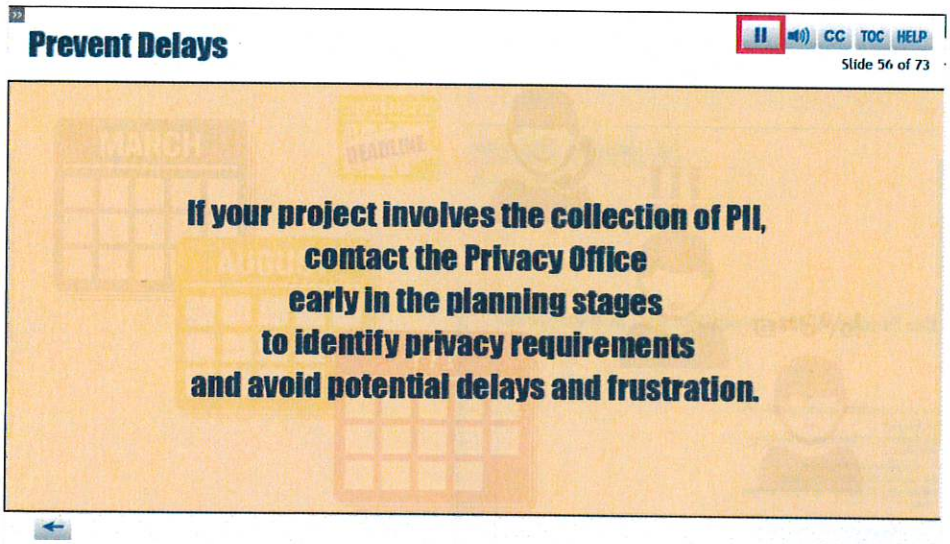
First, only disclose personal information to those who have a need to know and require the information

to perform their official duties.

Second, only use the information for official, work-related purposes.

Third, and most importantly, only grant access to PII when you're specifically authorized to do so.

Slide 58 - Prevent Delays



Slide notes

Now, let's review a common scenario and discuss how to avoid it.

Let's say your department has a big new project in the works.

Your business plan was approved in March, so you move toward your goal of implementation by the end of the fiscal year.

Five months in, things are looking good for an on-time delivery.

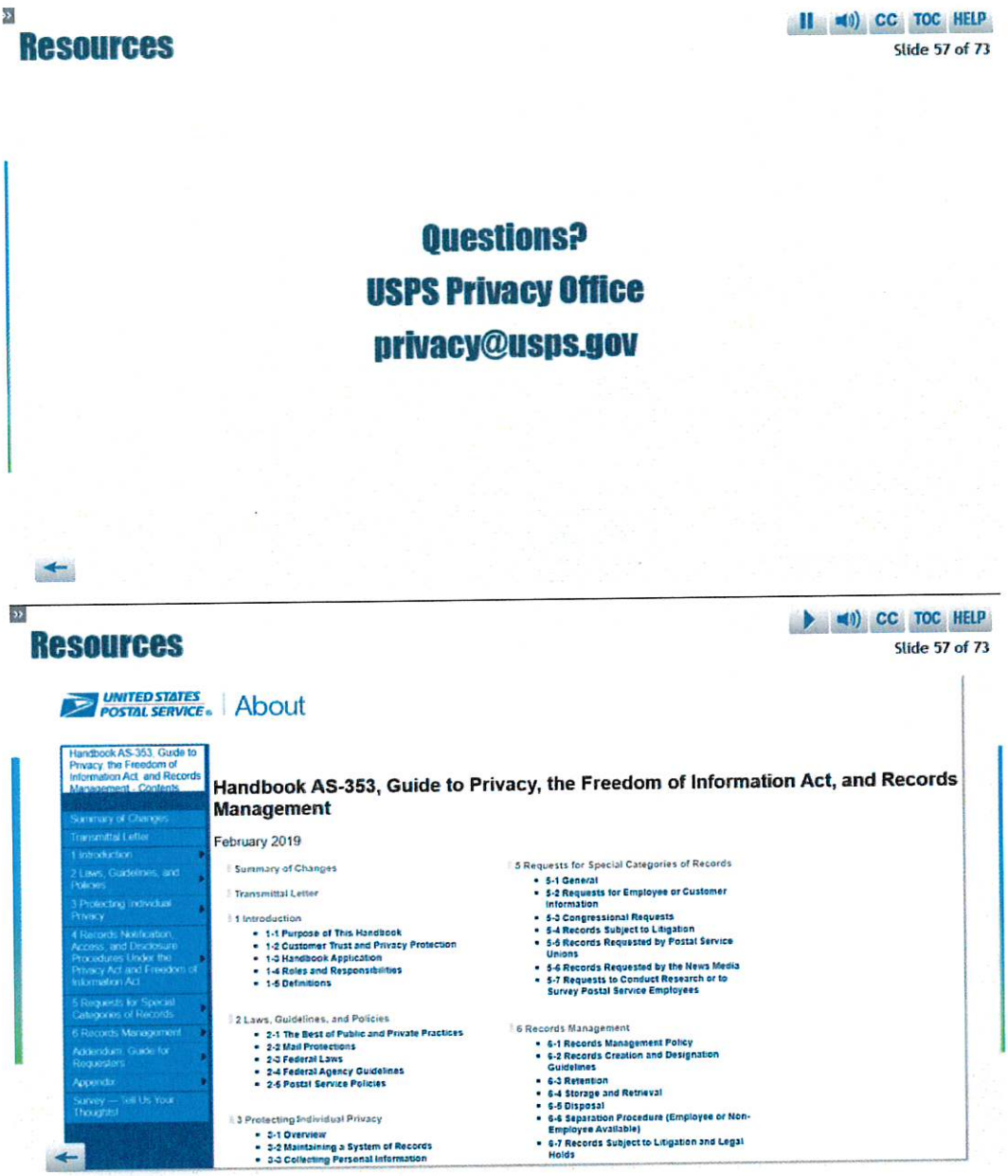
However, when legal reviews the plan, they notice you have not included privacy parameters or the SOR process.

As you learned in Module 1, creating or revising an SOR can take up to 8 months, which means your project is now behind schedule.

If your project requires the collection of PII, contact the Privacy Office early in the planning stages

to identify privacy requirements and avoid potential delays and frustration.

Slide 59 - Resources



Slide notes

Whenever you have questions regarding a Privacy Act Statement or the USPS privacy policy,

you are encouraged to contact the Privacy Office directly.

You can also find comprehensive policy details, definitions, and Privacy Act requirements

in Handbook AS-353, *Guide to Privacy, the Freedom of Information Act, and Records Management*.

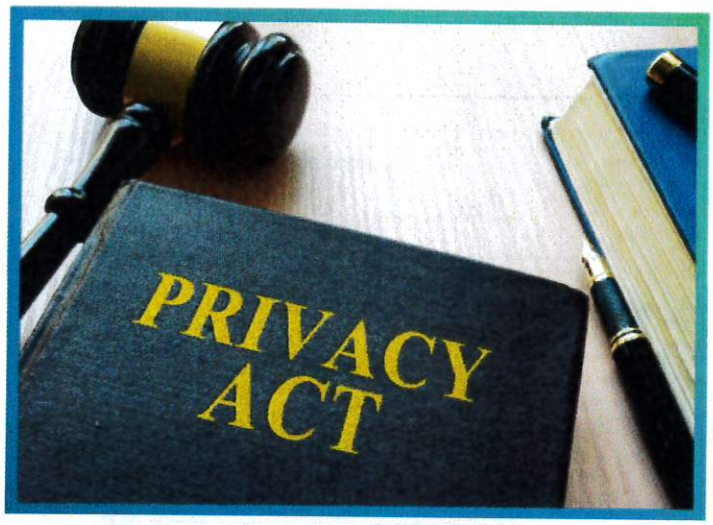
Several excerpts from AS-353 were used in this course for your reference. Find a link to this publication in the Help menu.

Slide 60 - Module 3 Summary

Module 3 Summary

CC TOC HELP

Slide 58 of 73



Module 3 Summary

CC TOC HELP

Slide 58 of 73

Physical

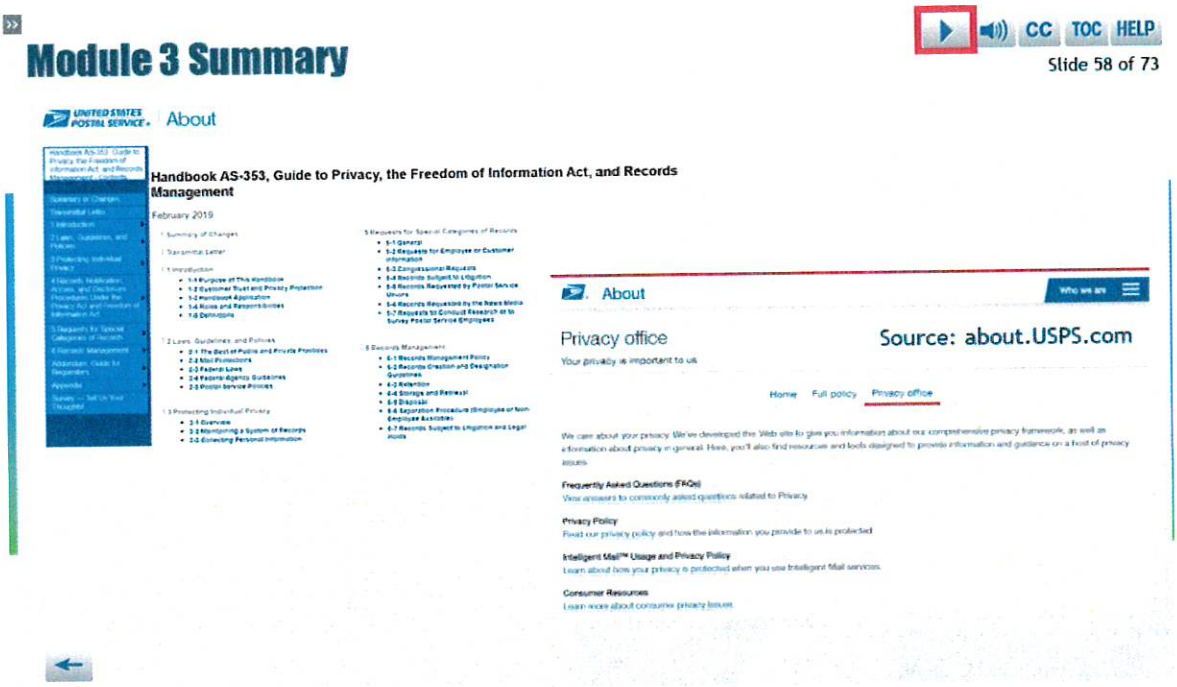
All Postal Service workstations and mobile computing devices must be protected, at minimum, by secure physical access to the facility or room.

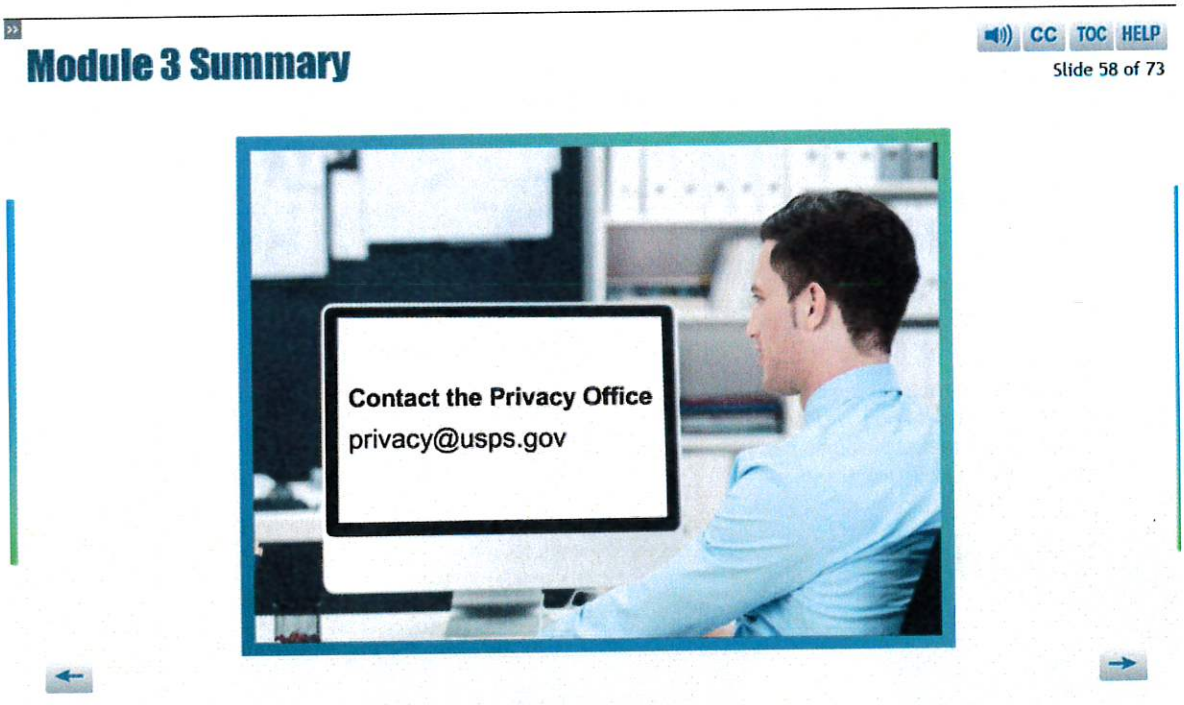
Administrative

Assure that policies and procedures, including those for security clearances and privacy and security training, are in place for the protection of PII.

Technical

Have technical safeguards, such as firewalls, access management, transmission security, and data encryption.





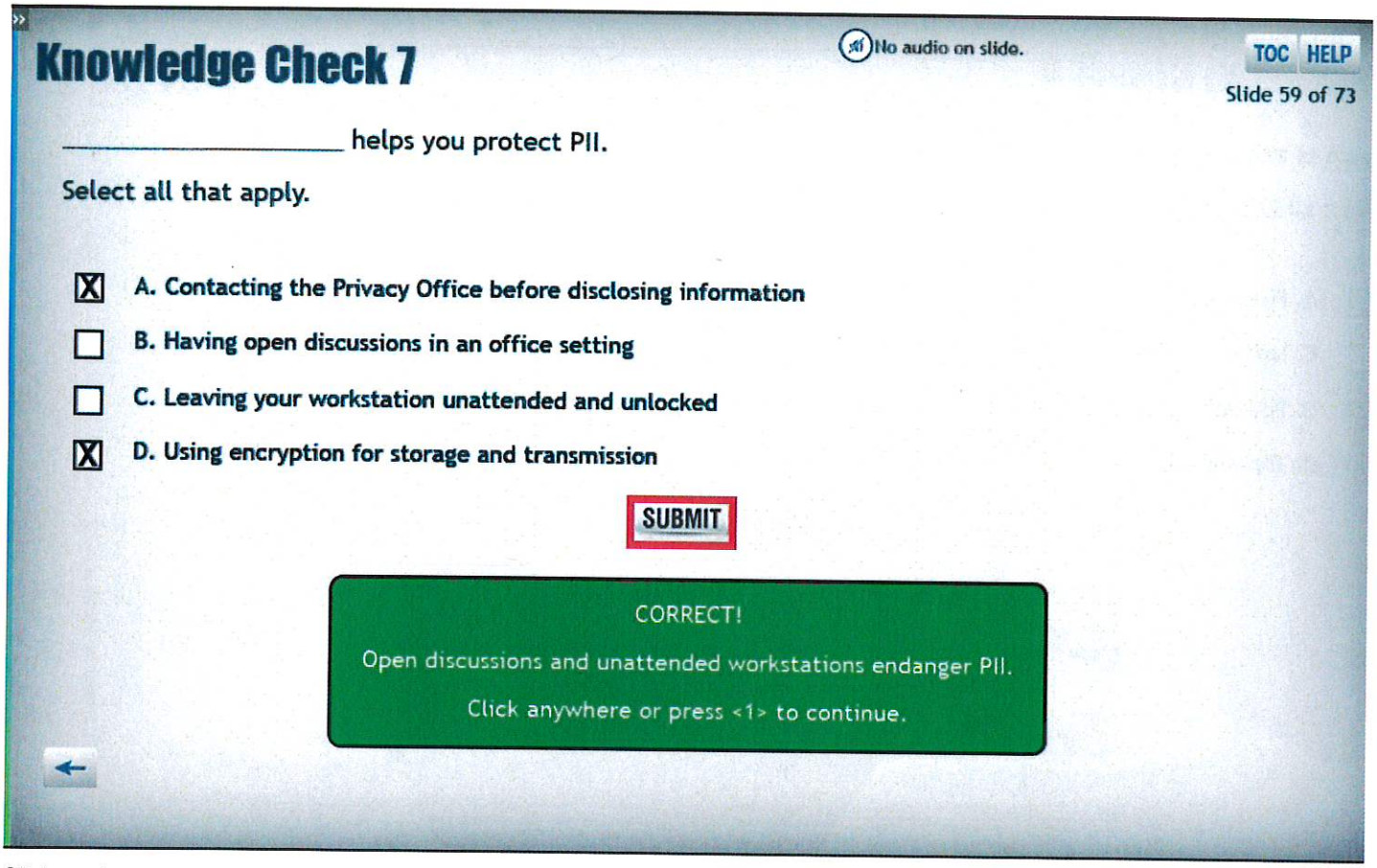
Slide notes

To review, USPS takes privacy very seriously.

We have multiple safeguards to ensure PII is collected, maintained, disclosed, and destroyed in a safe and secure manner.

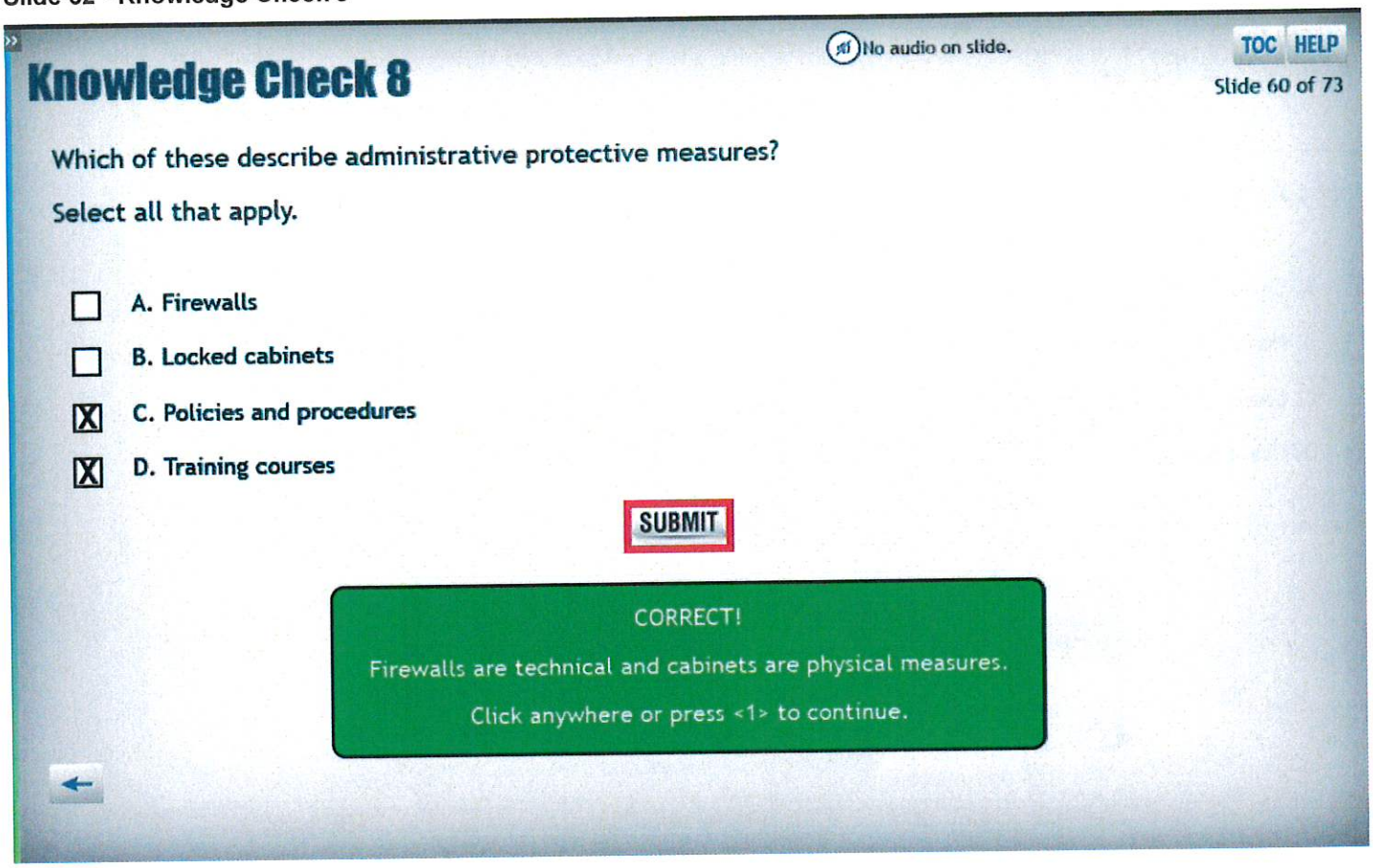
You have online resources available to help you stay in compliance, but remember, it's as easy as contacting the Privacy Office!

Slide 61 - Knowledge Check 7



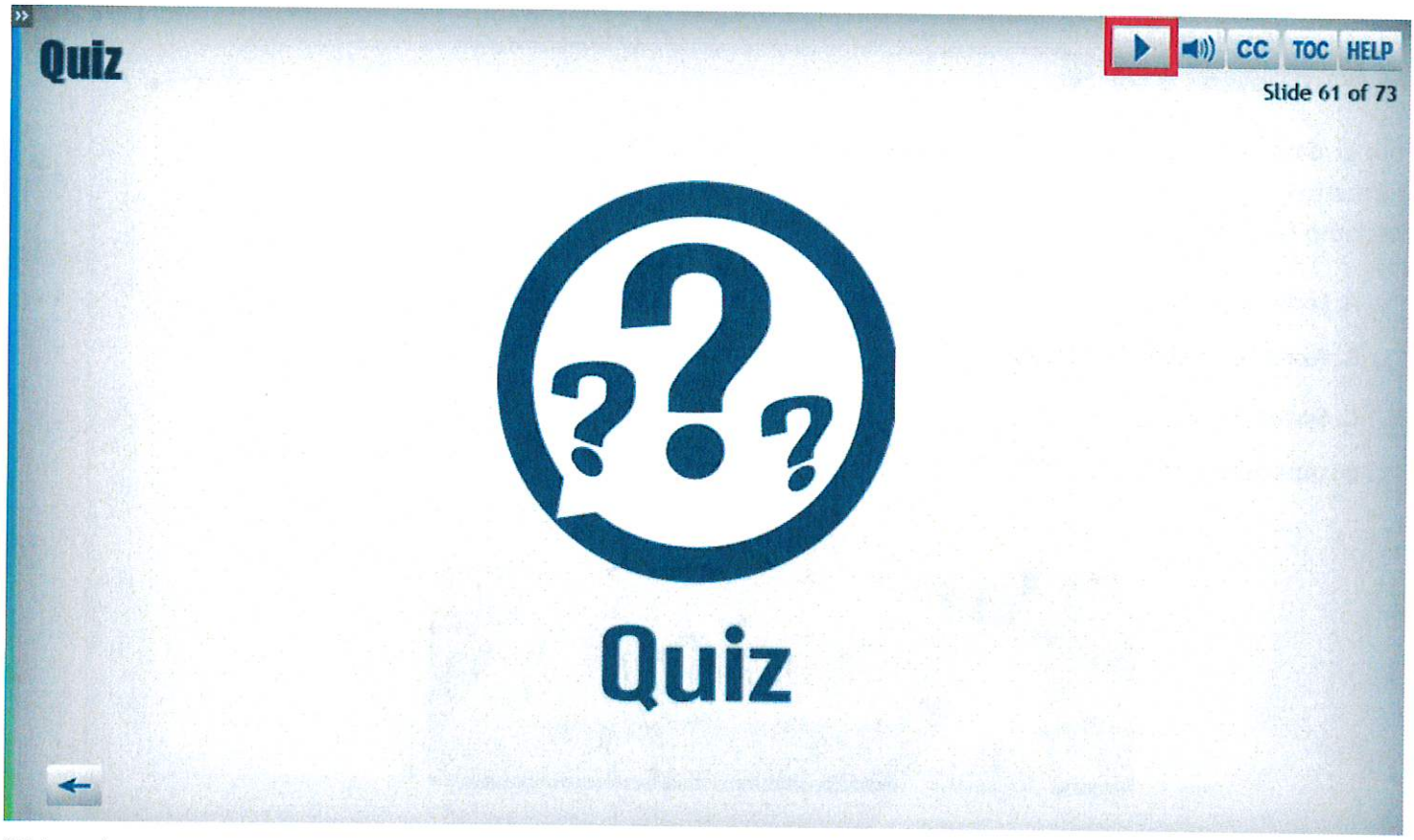
Slide notes

Slide 62 - Knowledge Check 8



Slide notes

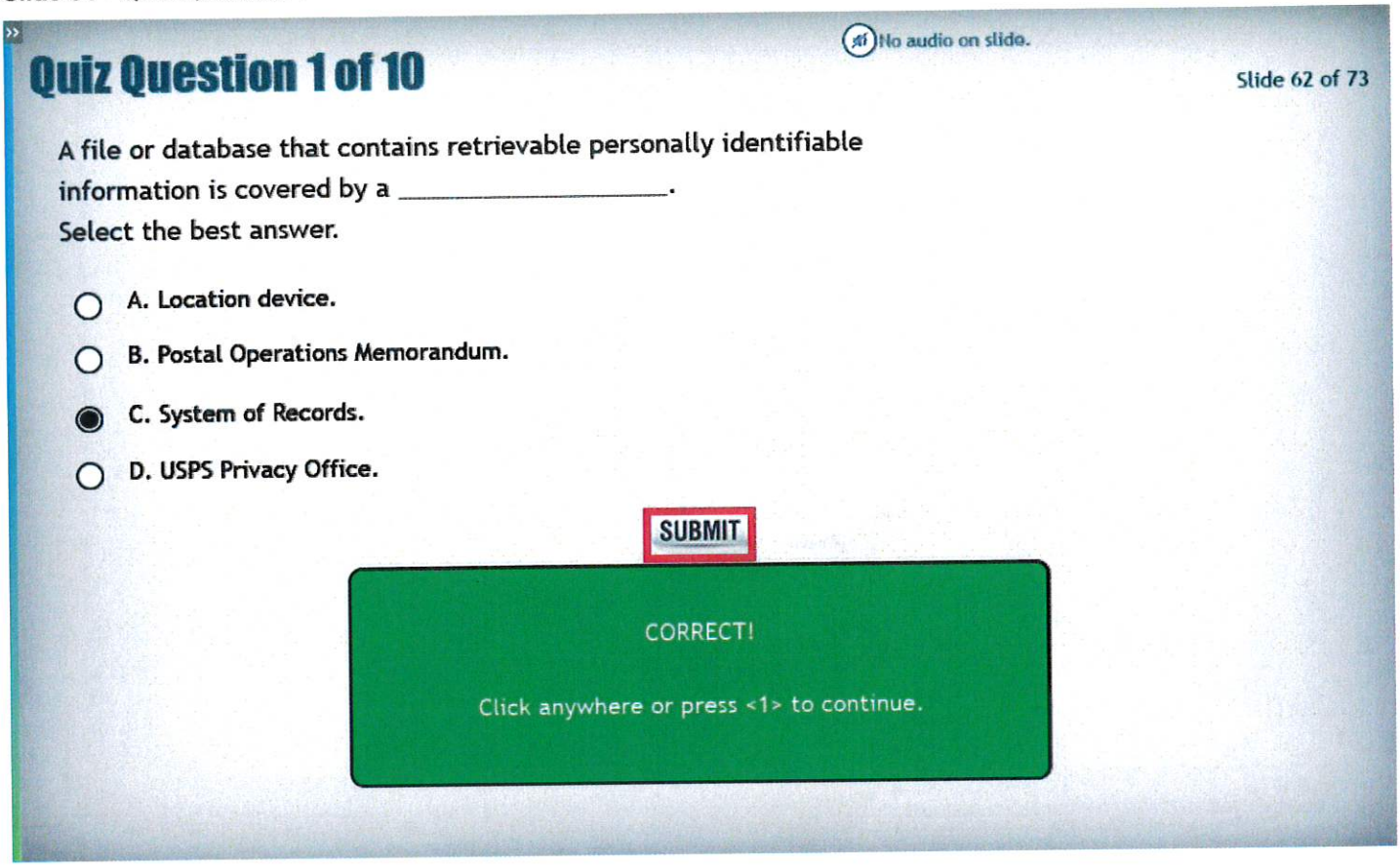
Slide 63 - Quiz



Slide notes

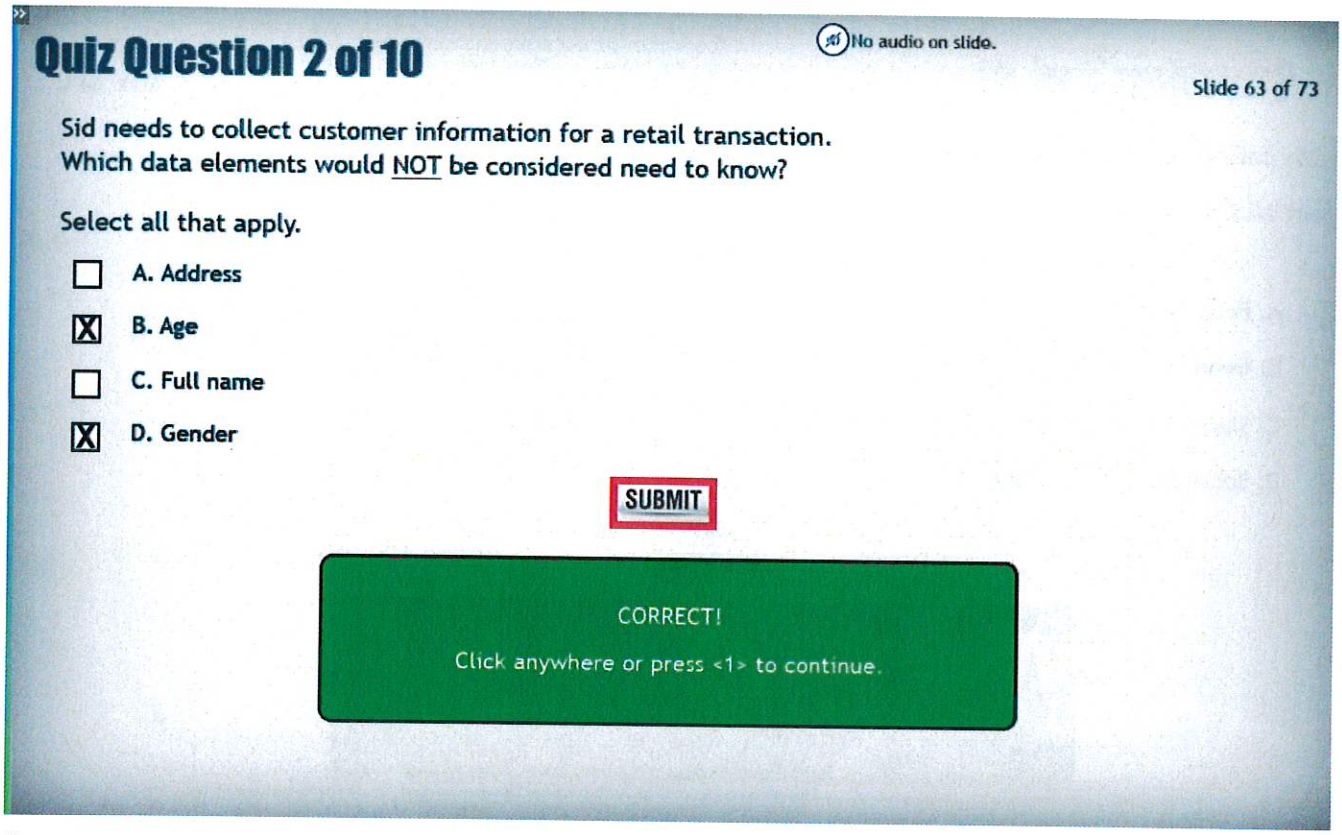
Now, it's time to test your knowledge. Eighty percent is passing. Good luck!

Slide 64 - Quiz Question 1



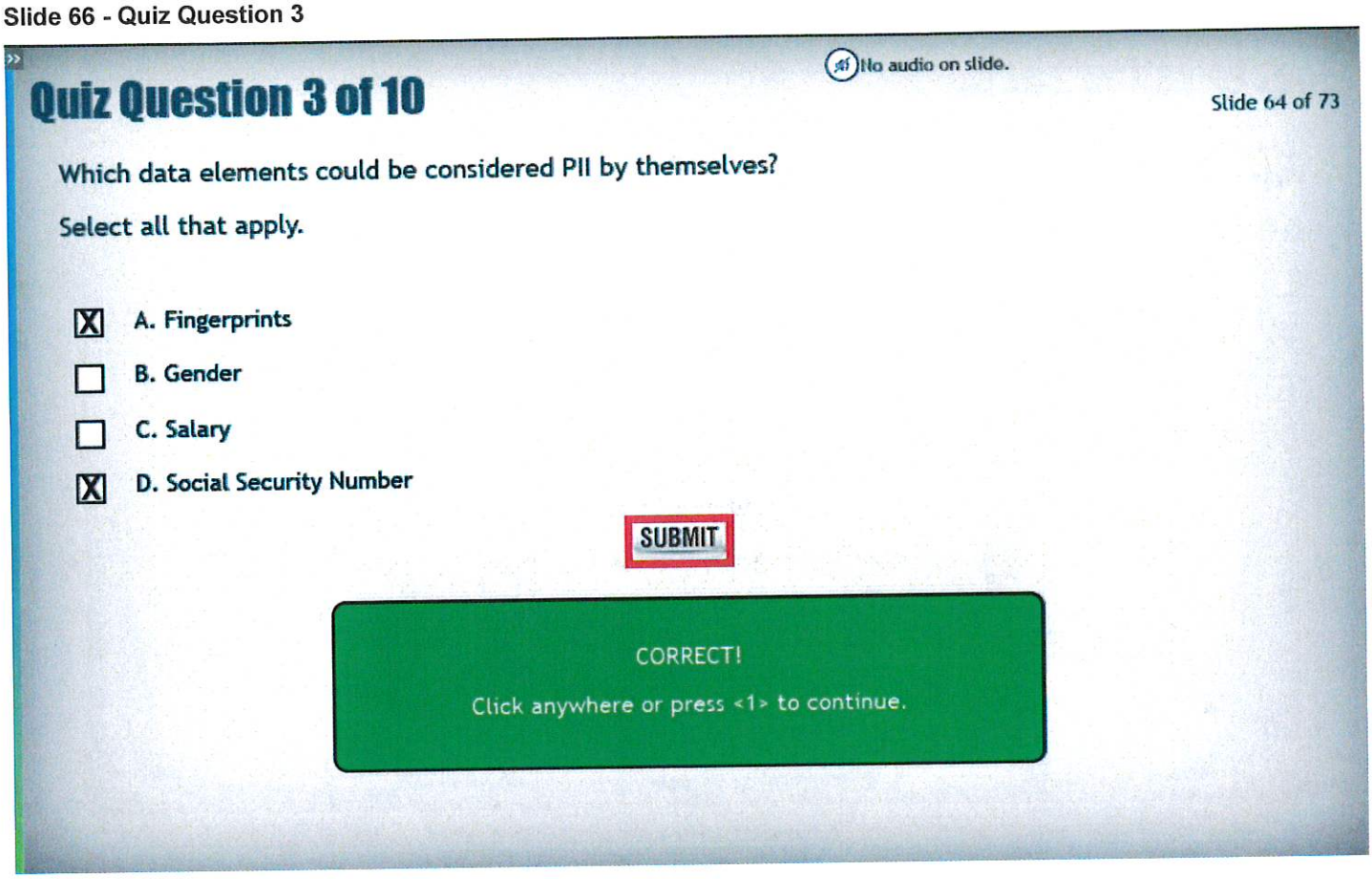
Slide notes

Slide 65 - Quiz Question 2



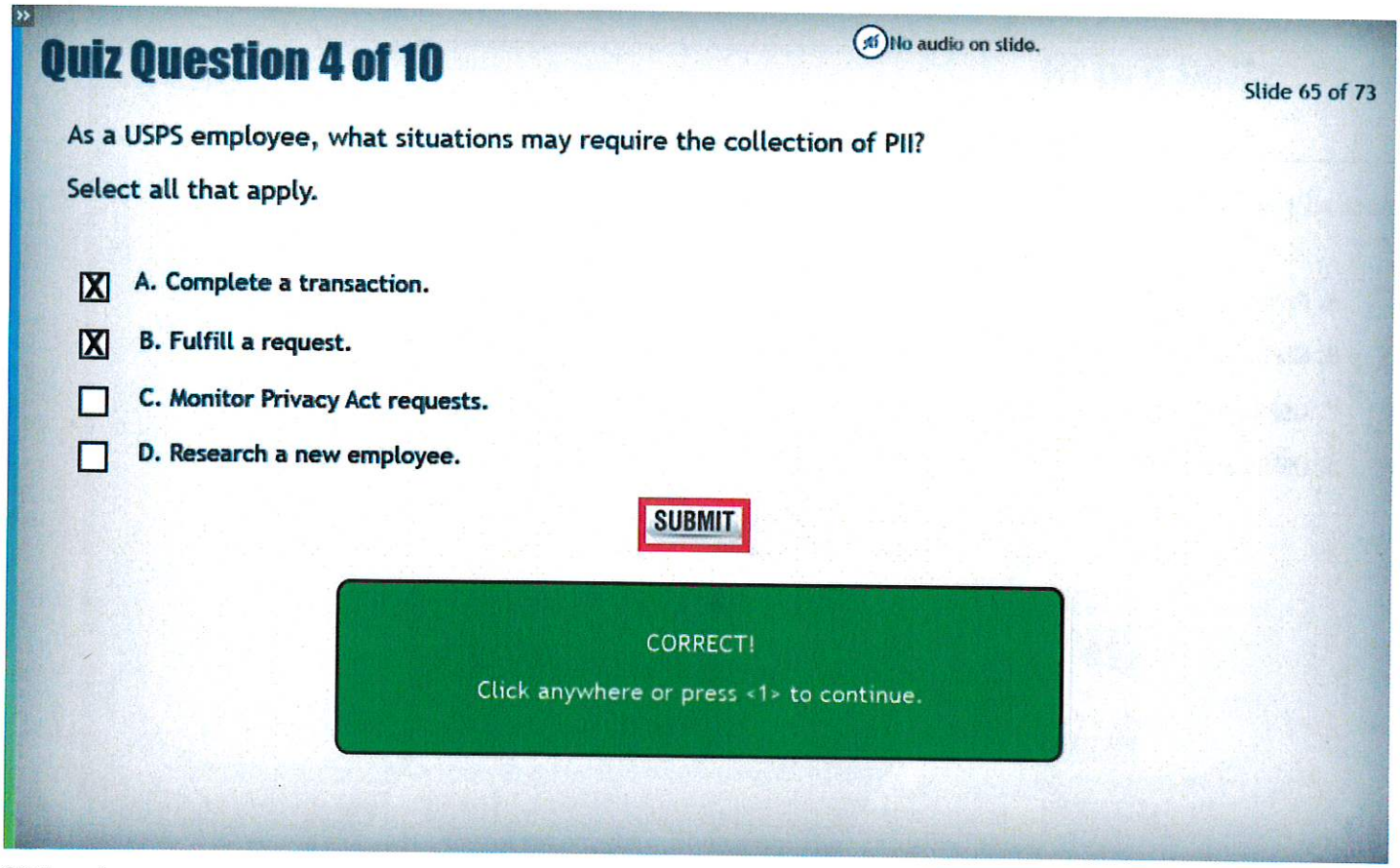
Slide notes

Slide 66 - Quiz Question 3



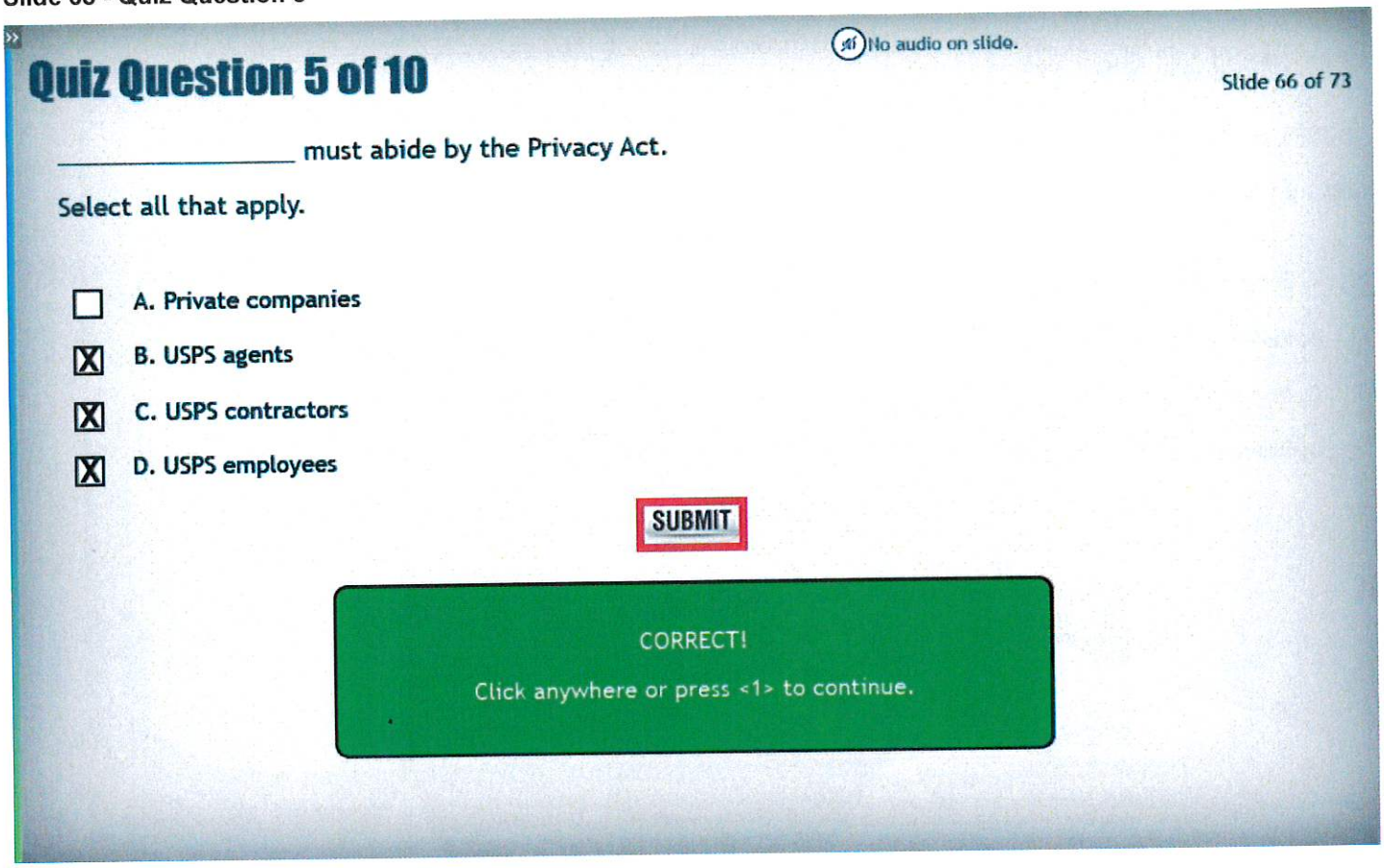
Slide notes

Slide 67 - Quiz Question 4



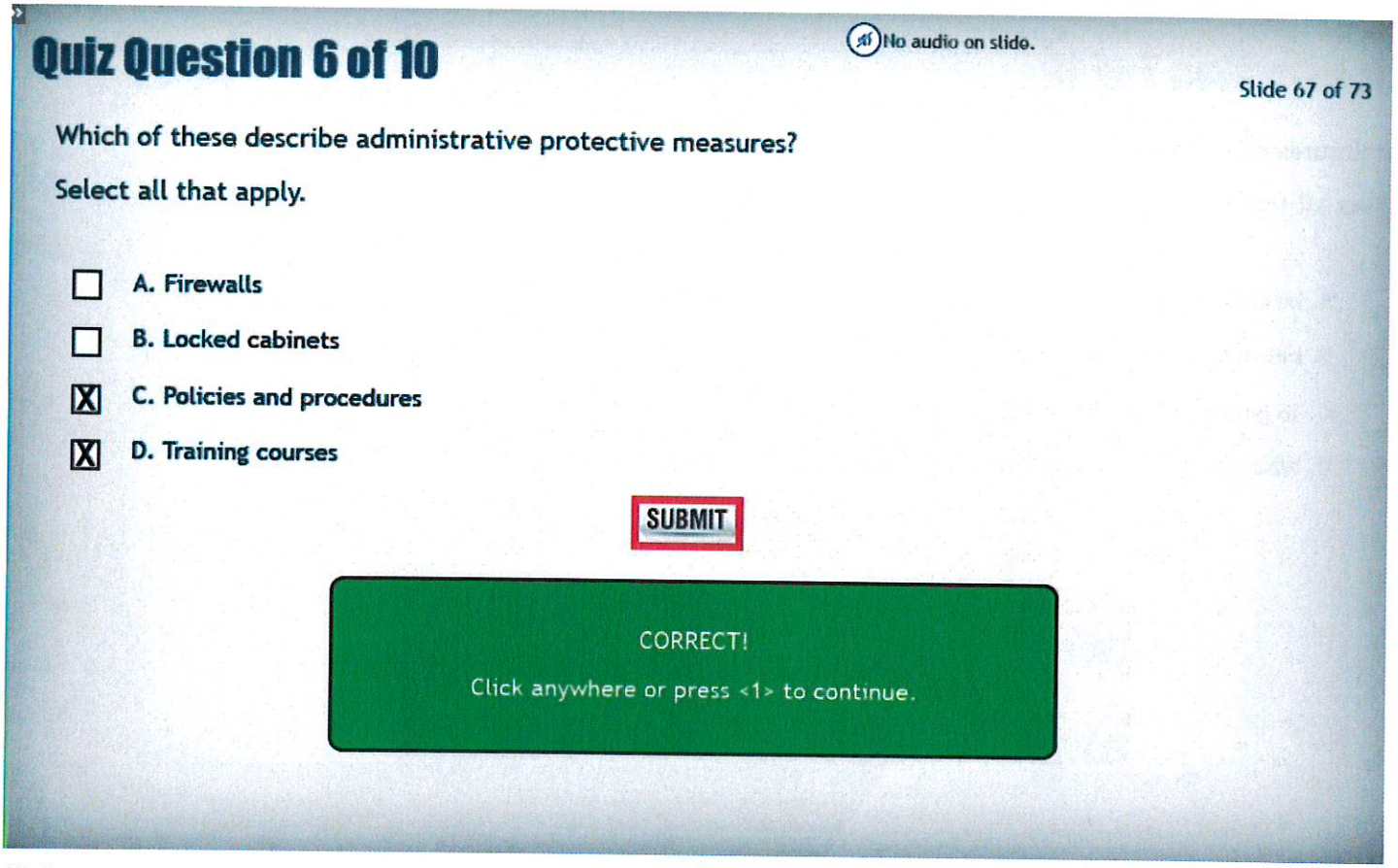
Slide notes

Slide 68 - Quiz Question 5



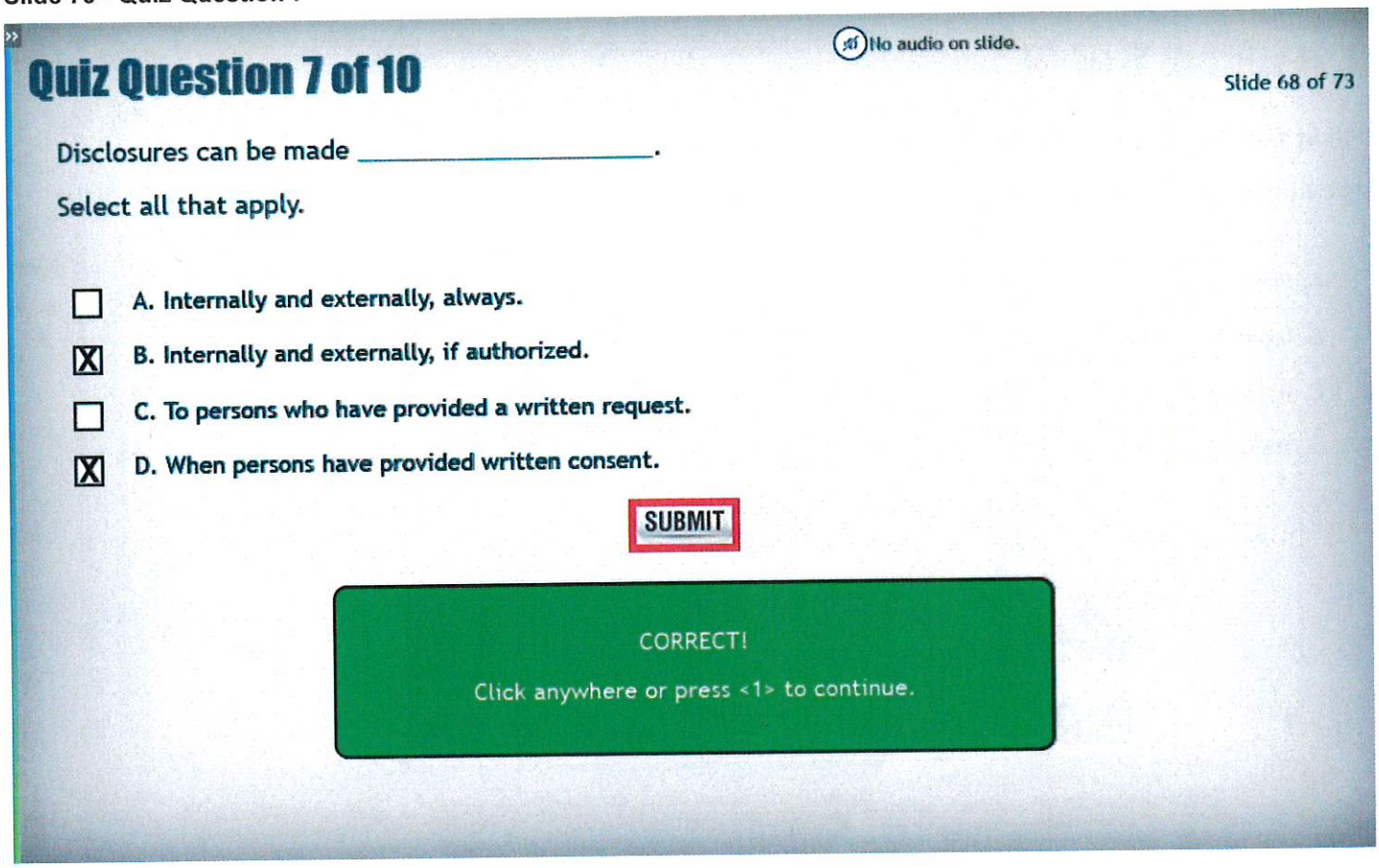
Slide notes

Slide 69 - Quiz Question 6



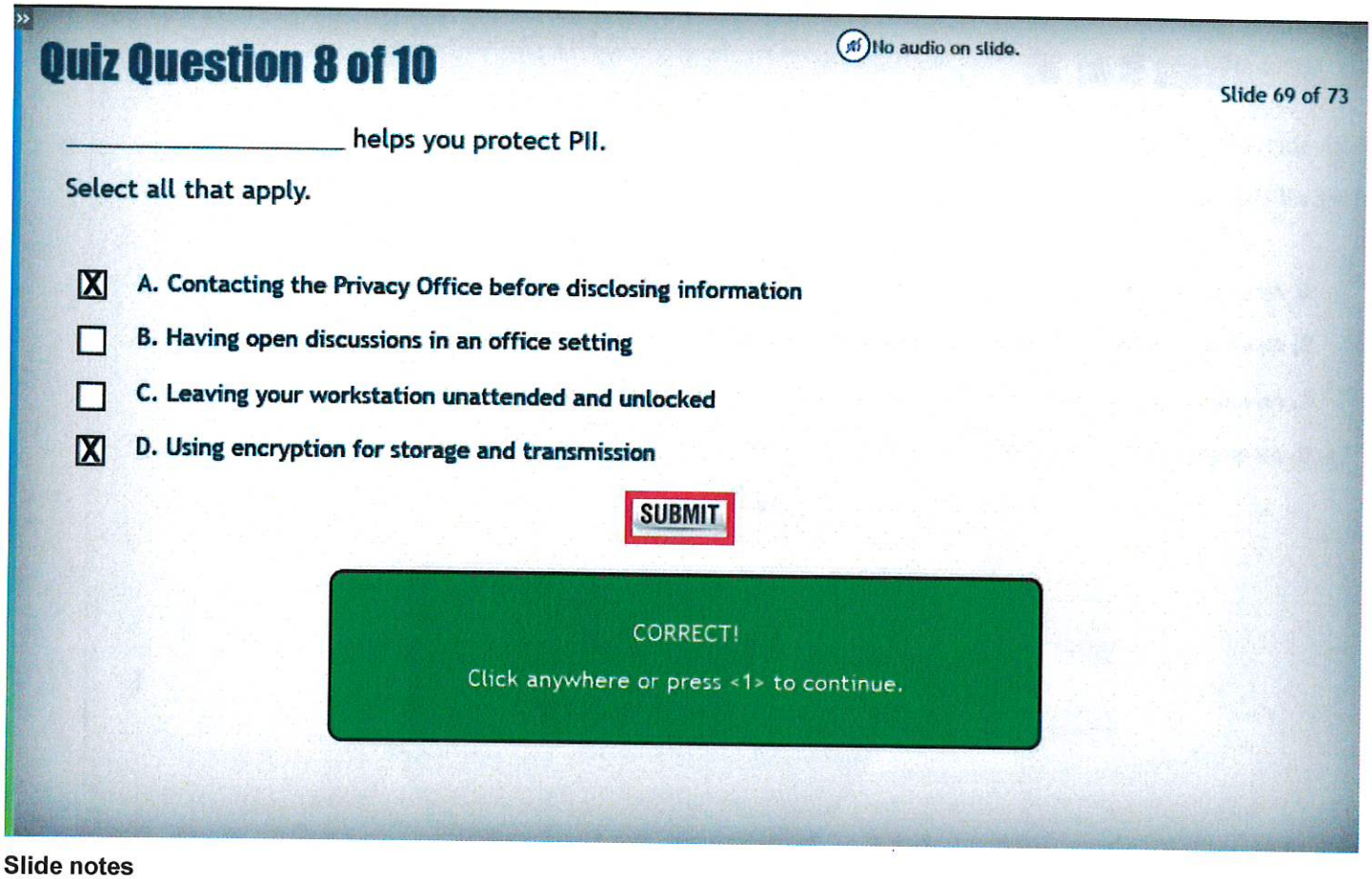
Slide notes

Slide 70 - Quiz Question 7



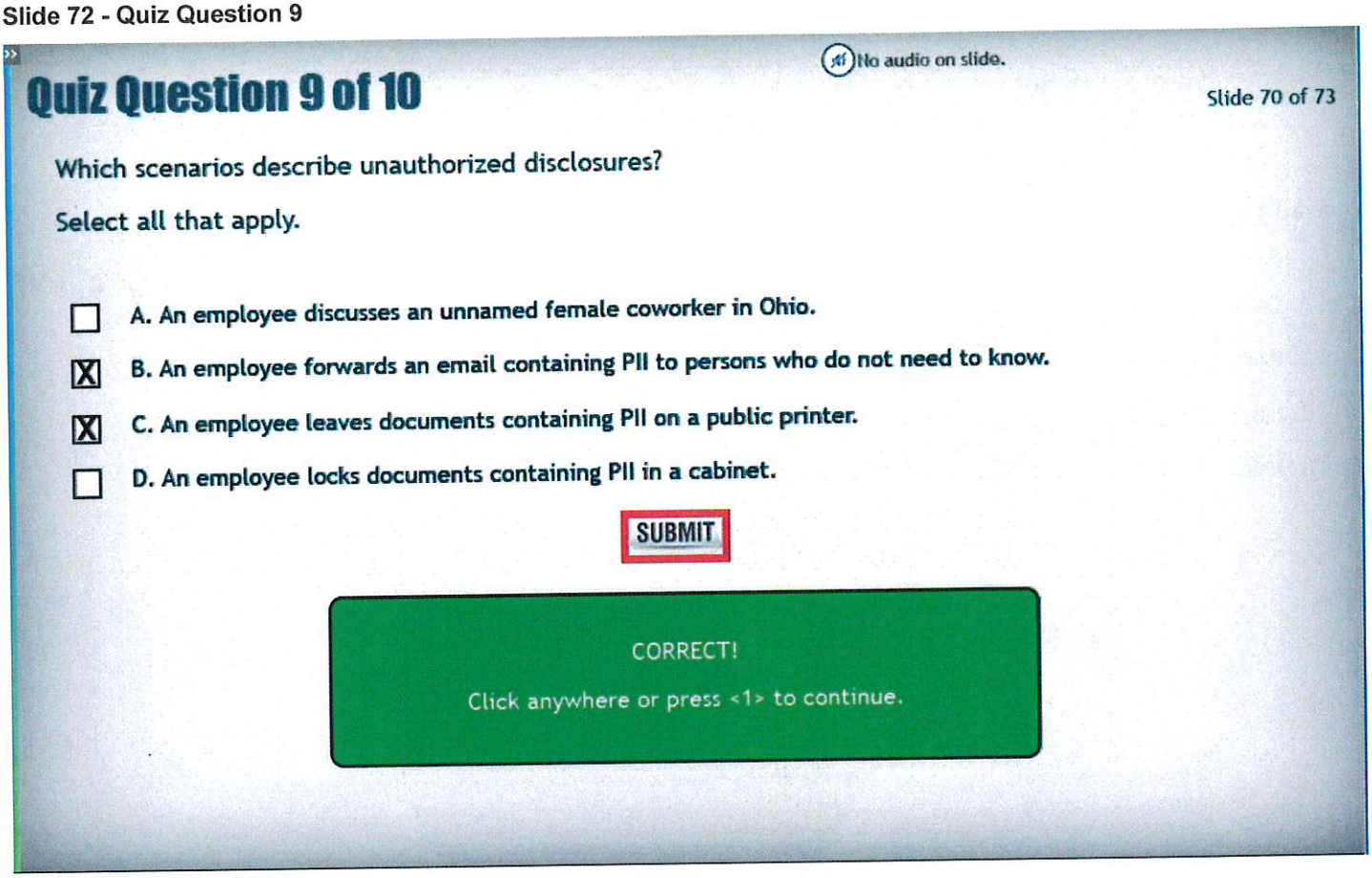
Slide notes

Slide 71 - Quiz Question 8



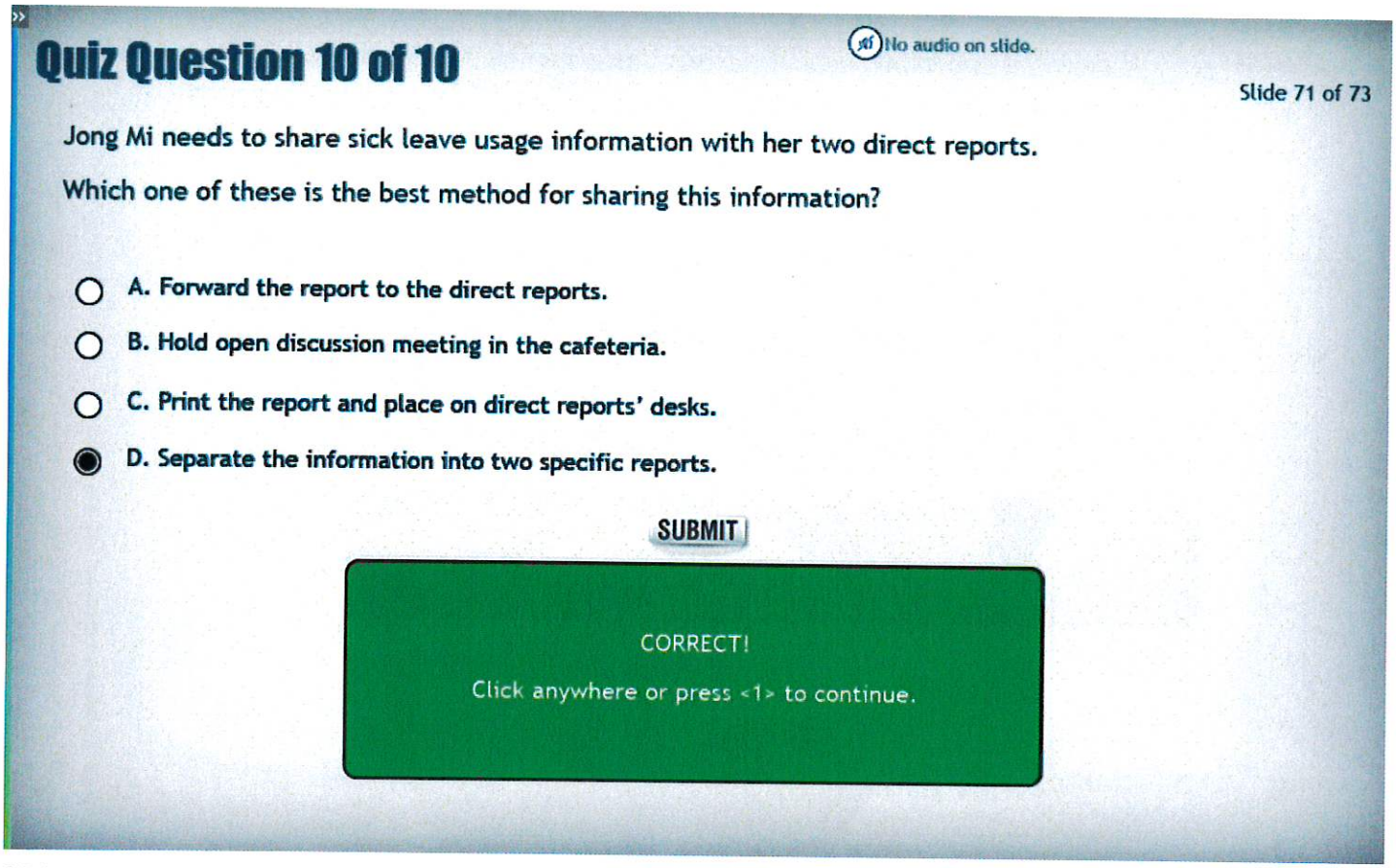
Slide notes

Slide 72 - Quiz Question 9



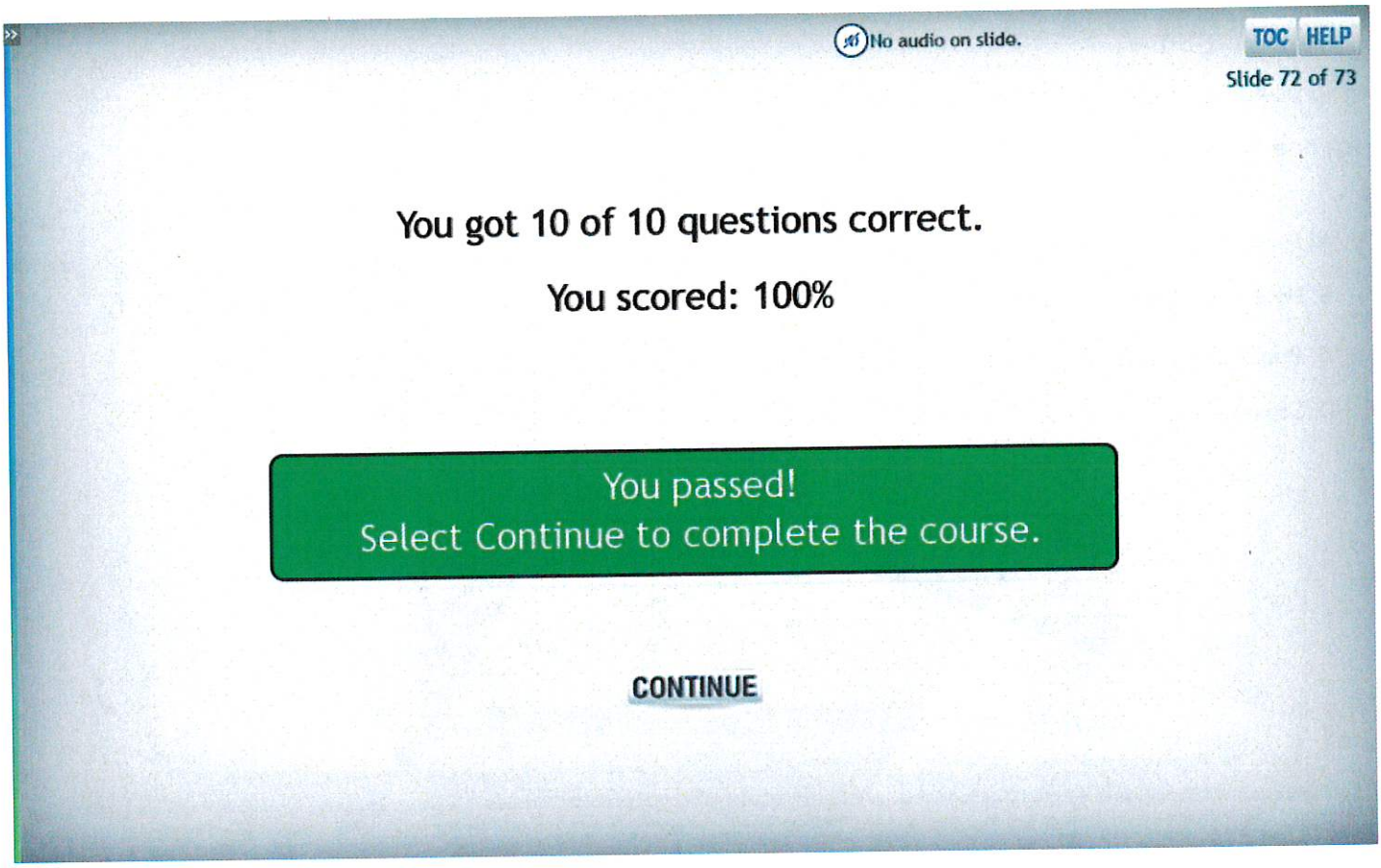
Slide notes

Slide 73 - Quiz Question 10



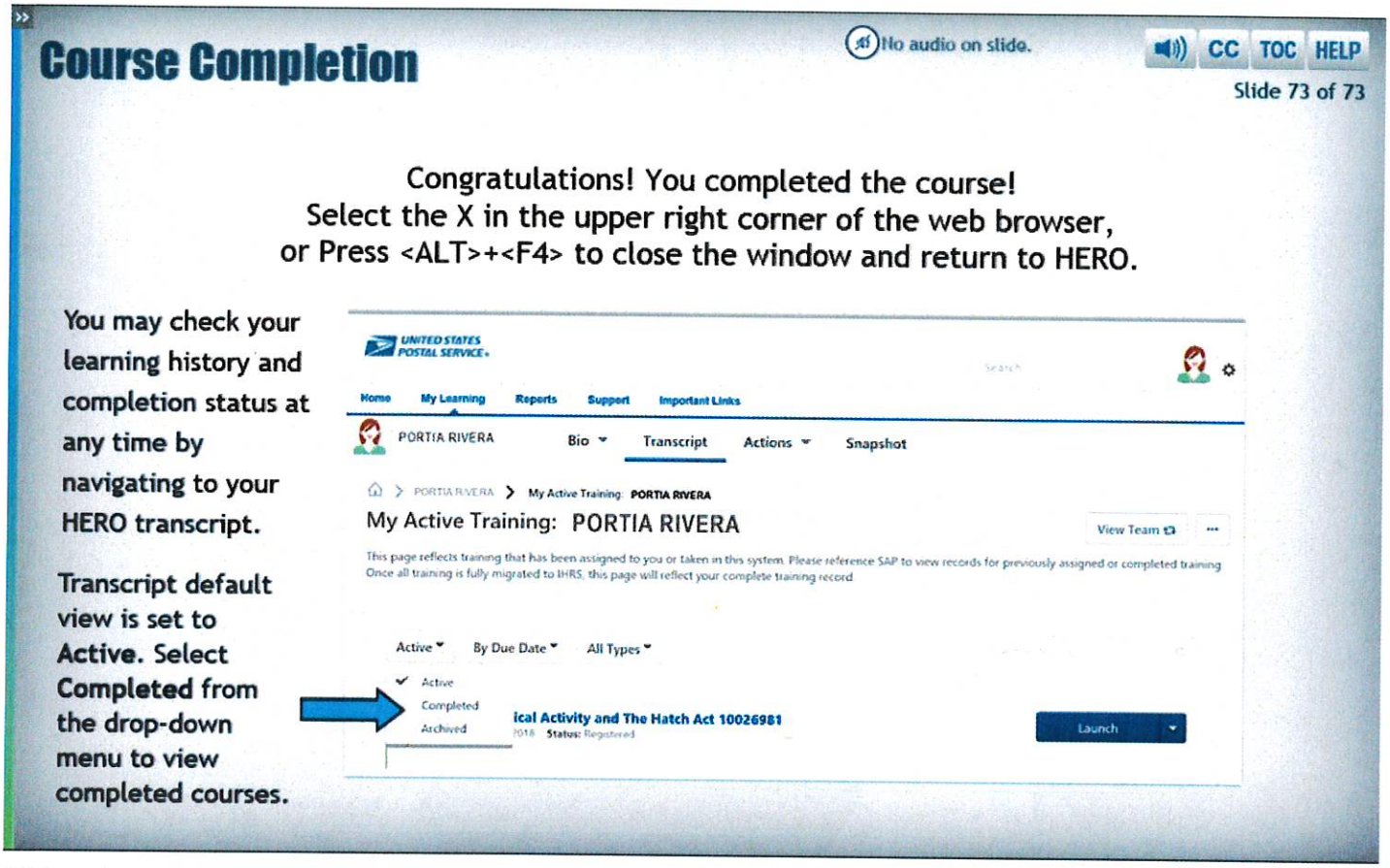
Slide notes

Slide 74 - Assessment Results



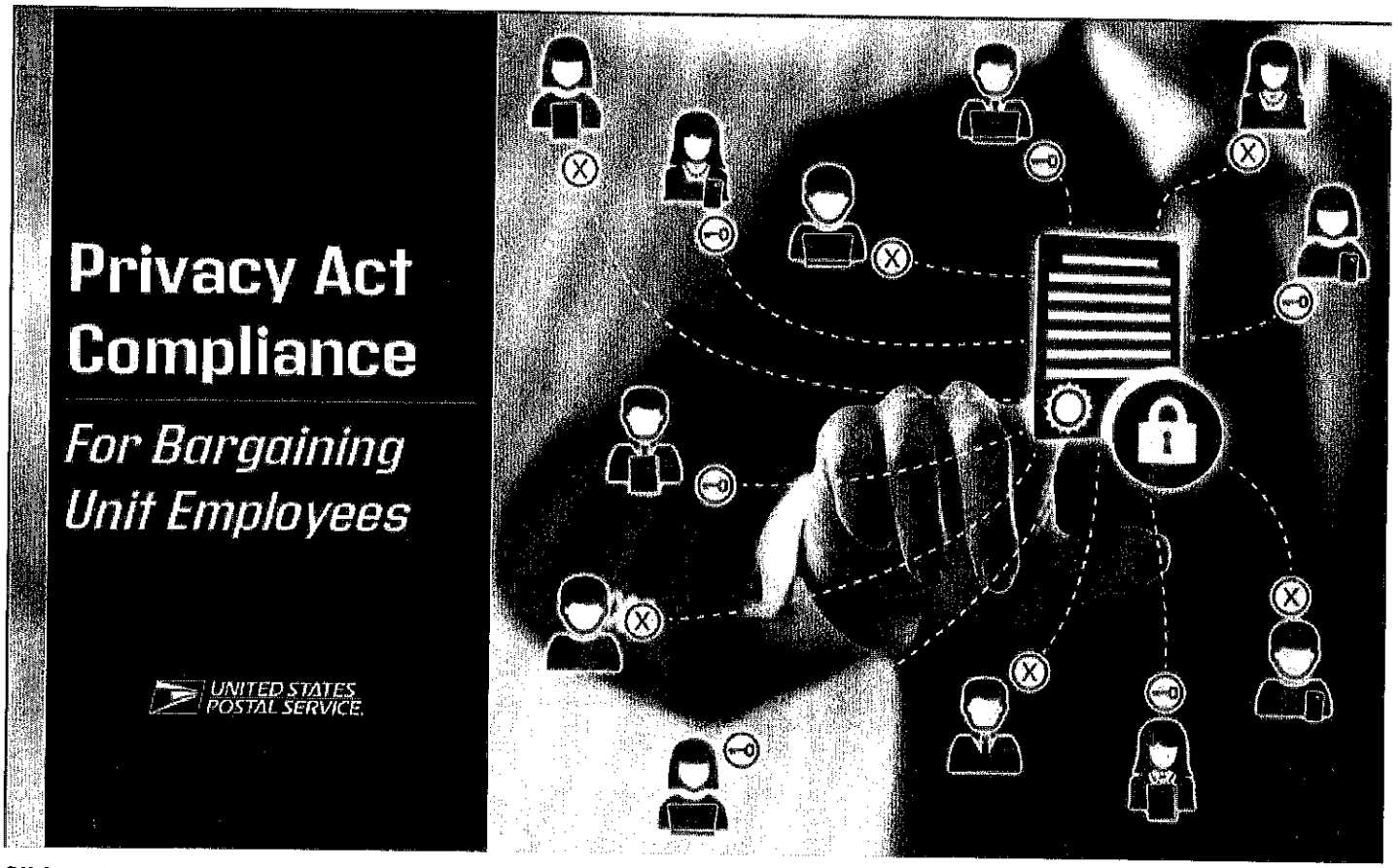
Slide notes

Slide 75 - Course Completion



Slide notes

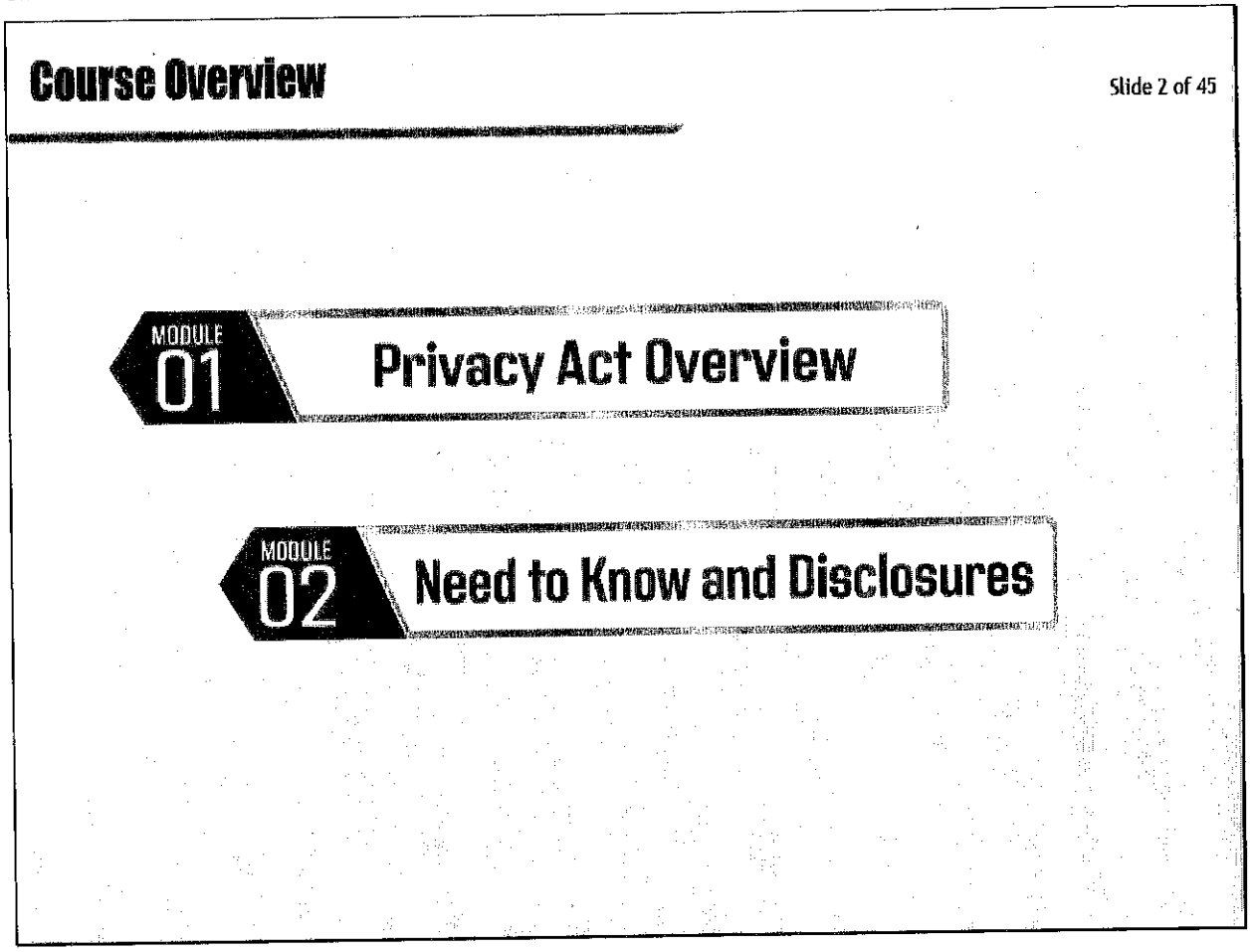
Slide 1 - Welcome



Slide notes

Welcome to the Privacy Act Compliance training course.

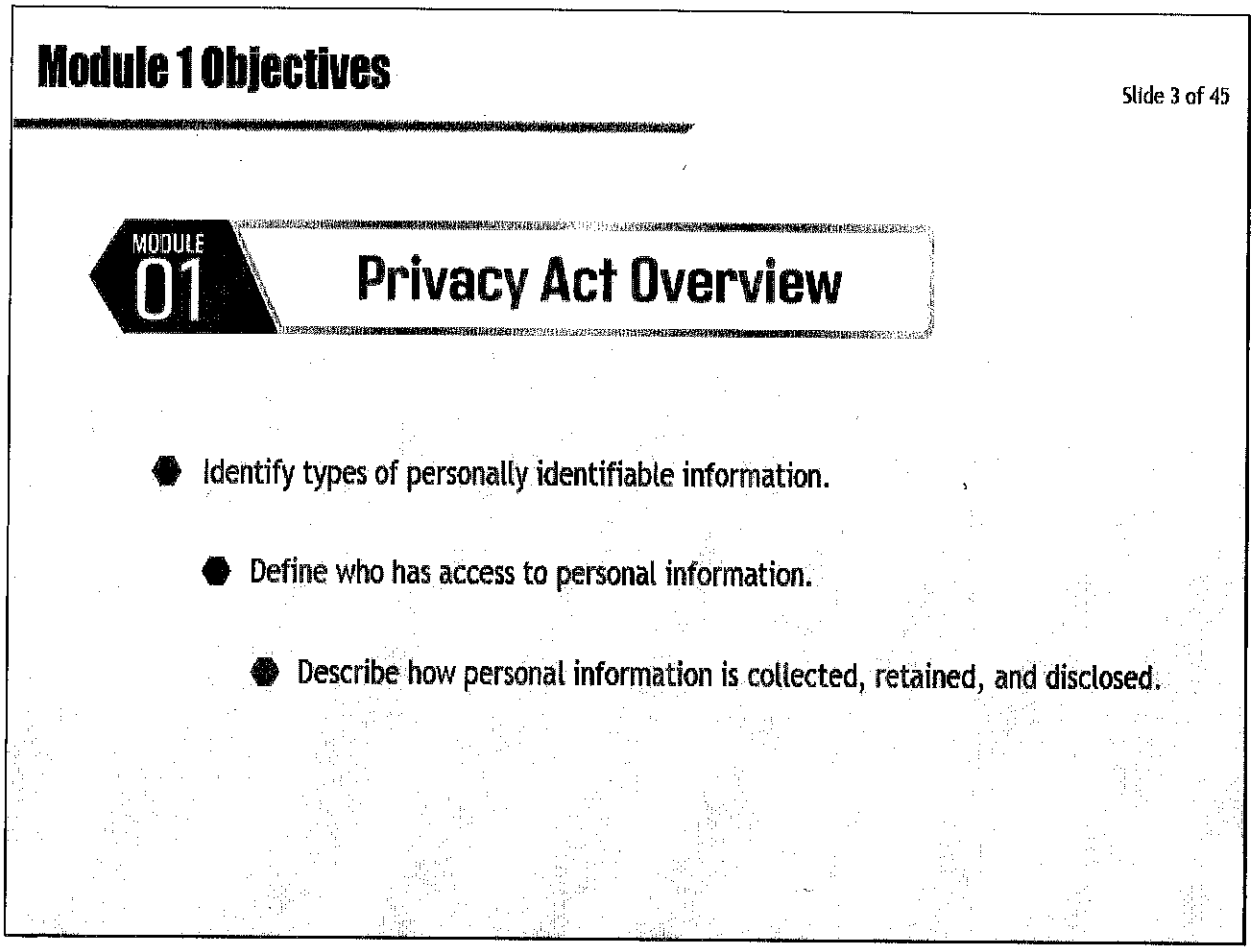
Slide 2 - Course Overview



Slide notes

This course aims to improve your familiarity with requirements of the Privacy Act, responsibilities for compliance, and implications of noncompliance in the Postal Service workplace.

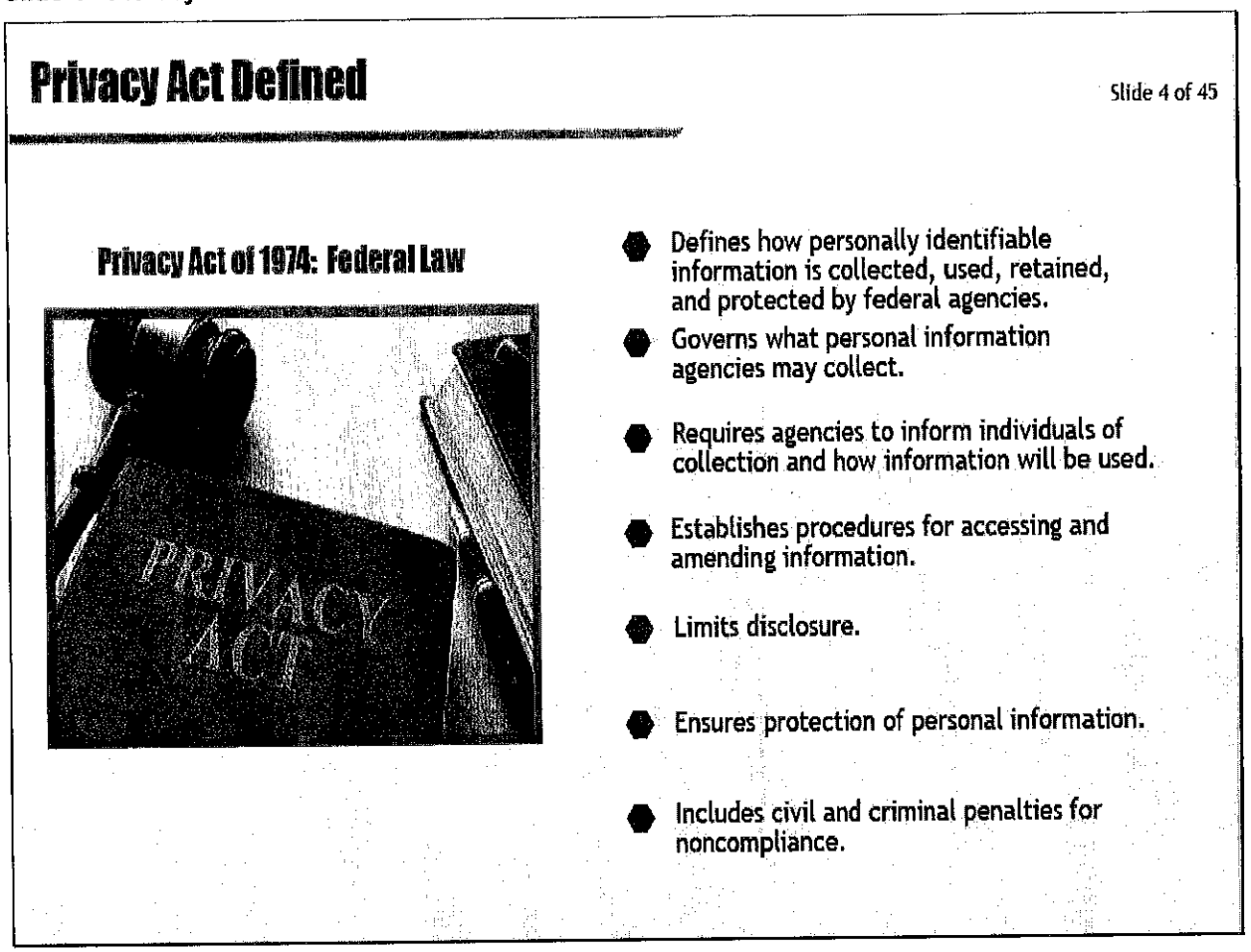
Slide 3 - Module 1 Objectives



Slide notes

Welcome to Module 1, Privacy Act Overview. By the end of this module, you should be able to identify types of personally identifiable information, define who has access to personal information, and describe how personal information is collected, retained, and disclosed.

Slide 4 - Privacy Act Defined

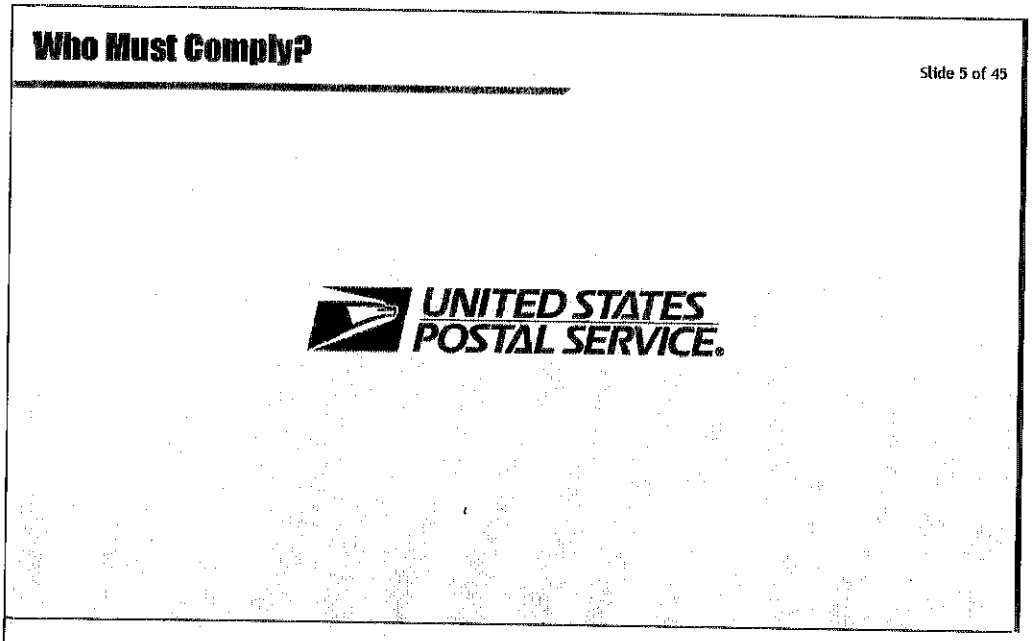


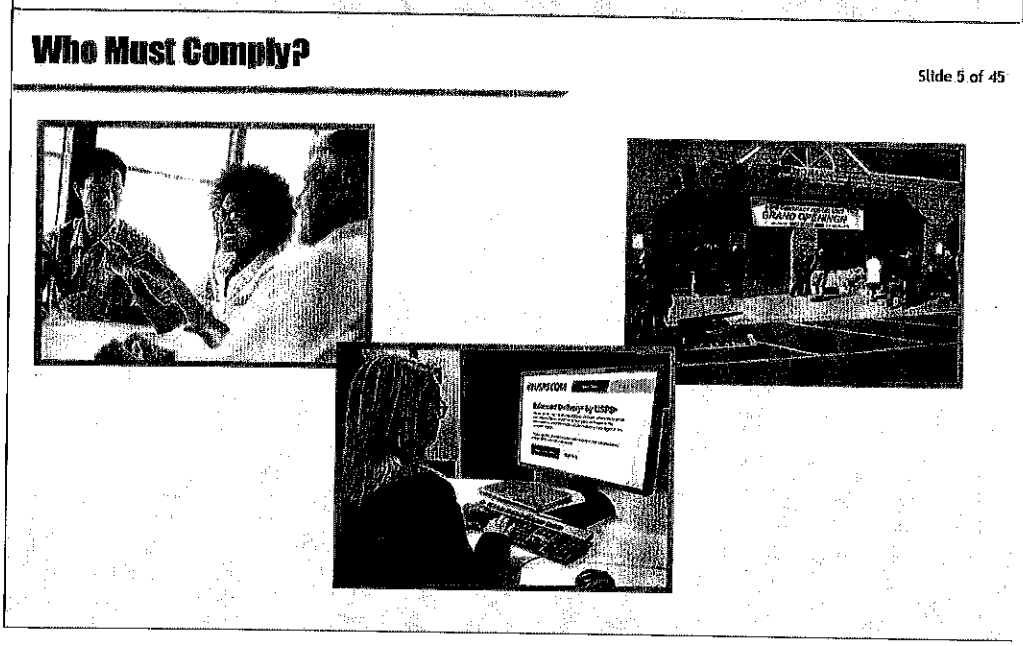
Slide notes

Let's start by defining our topic.

The Privacy Act of 1974 is a federal law that defines how personally identifiable information is collected, used, retained, and protected by federal agencies. The act governs the personal information agencies may collect and requires agencies to inform individuals of the collection and also how their information will be used. The act establishes procedures for an individual to access and amend their information, limits disclosure, ensures protection of the information, and includes civil and criminal penalties for noncompliance.

Slide 5 - Who Must Comply?





Slide notes

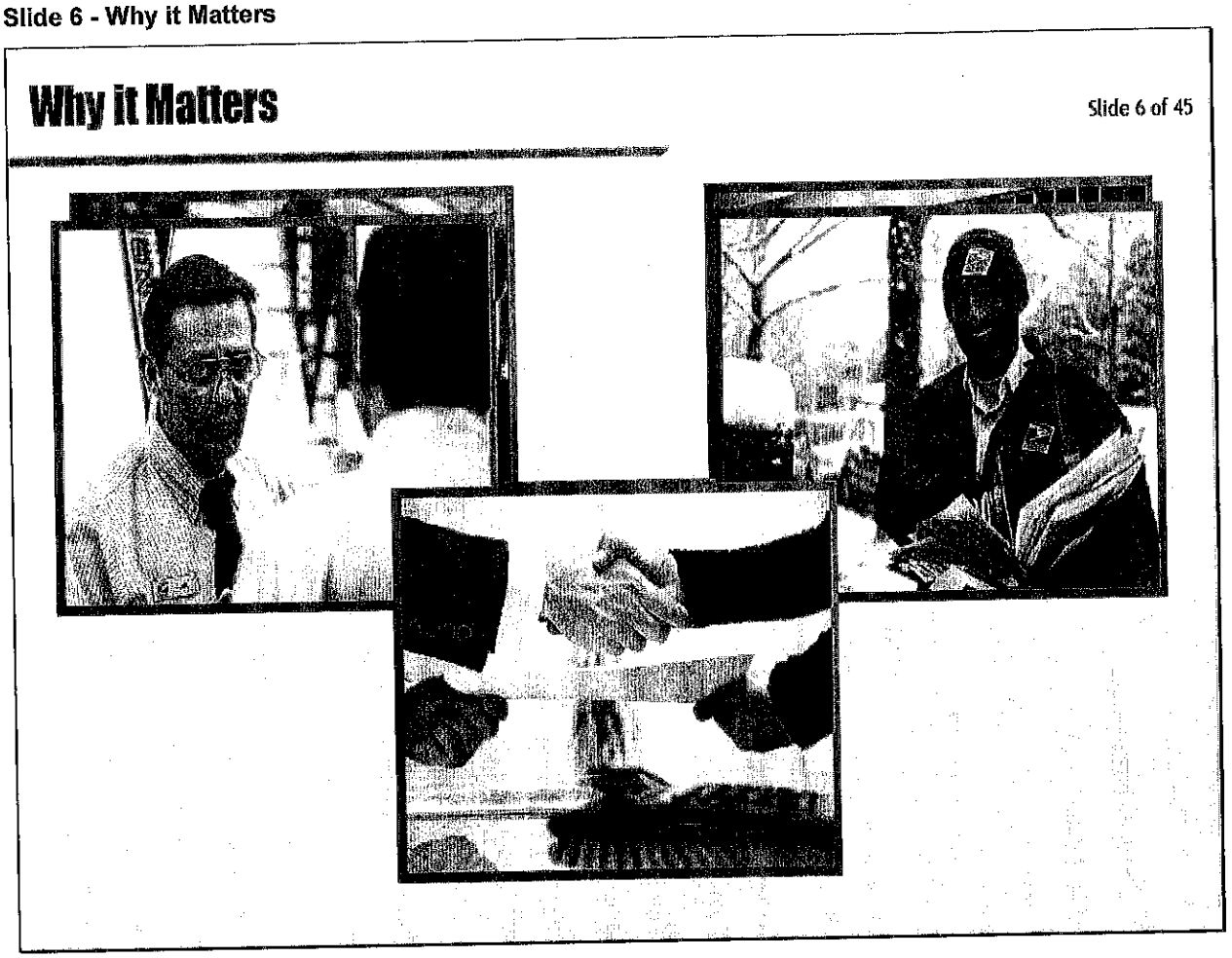
The Privacy Act applies to federal agencies in the public sector, including USPS, but does not apply to businesses in the private sector.

However, agents, contractors, and suppliers who help build or conduct USPS business operations,

and who have access to customer, employee, or other individuals' information,

must also abide by the Privacy Act and USPS privacy policies.

Slide 6 - Why it Matters



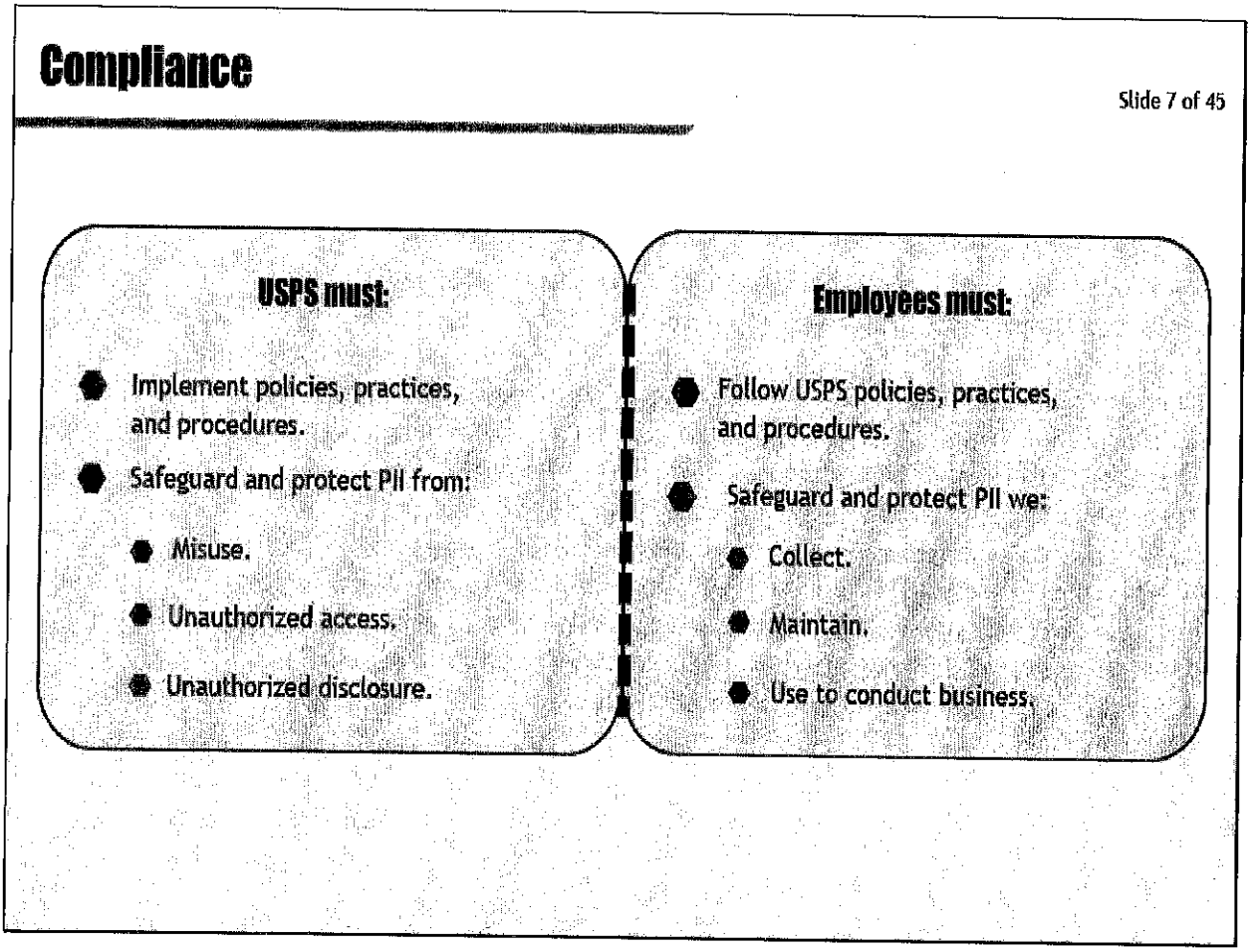
Slide notes

You may be wondering, why does the Privacy Act matter to me?

It matters because as a USPS employee, you play an important role in safeguarding the confidentiality and integrity of personal information.

Customers and employees depend on USPS as a trusted brand to protect the personal information they have agreed to share with us.

Slide 7 - Compliance



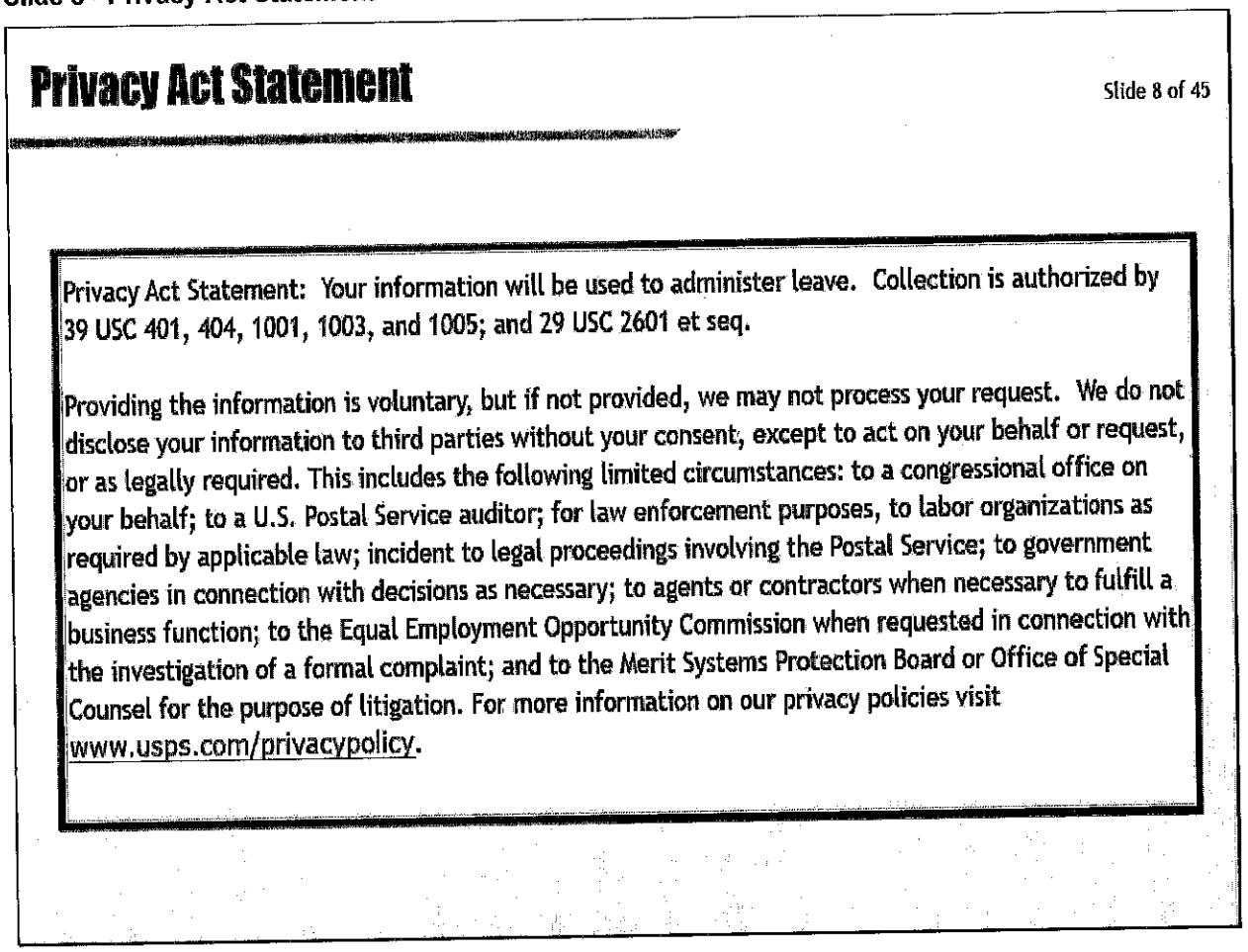
Slide notes

Now are you wondering how to comply?

First, USPS must implement policies, practices, and procedures to safeguard and protect personal information from misuse, unauthorized access, and unauthorized disclosure.

Second, all USPS employees, including you, must follow established USPS policies, practices, and procedures to safeguard and protect the PII we collect, maintain, and use to conduct business.

Slide 8 - Privacy Act Statement



Slide notes

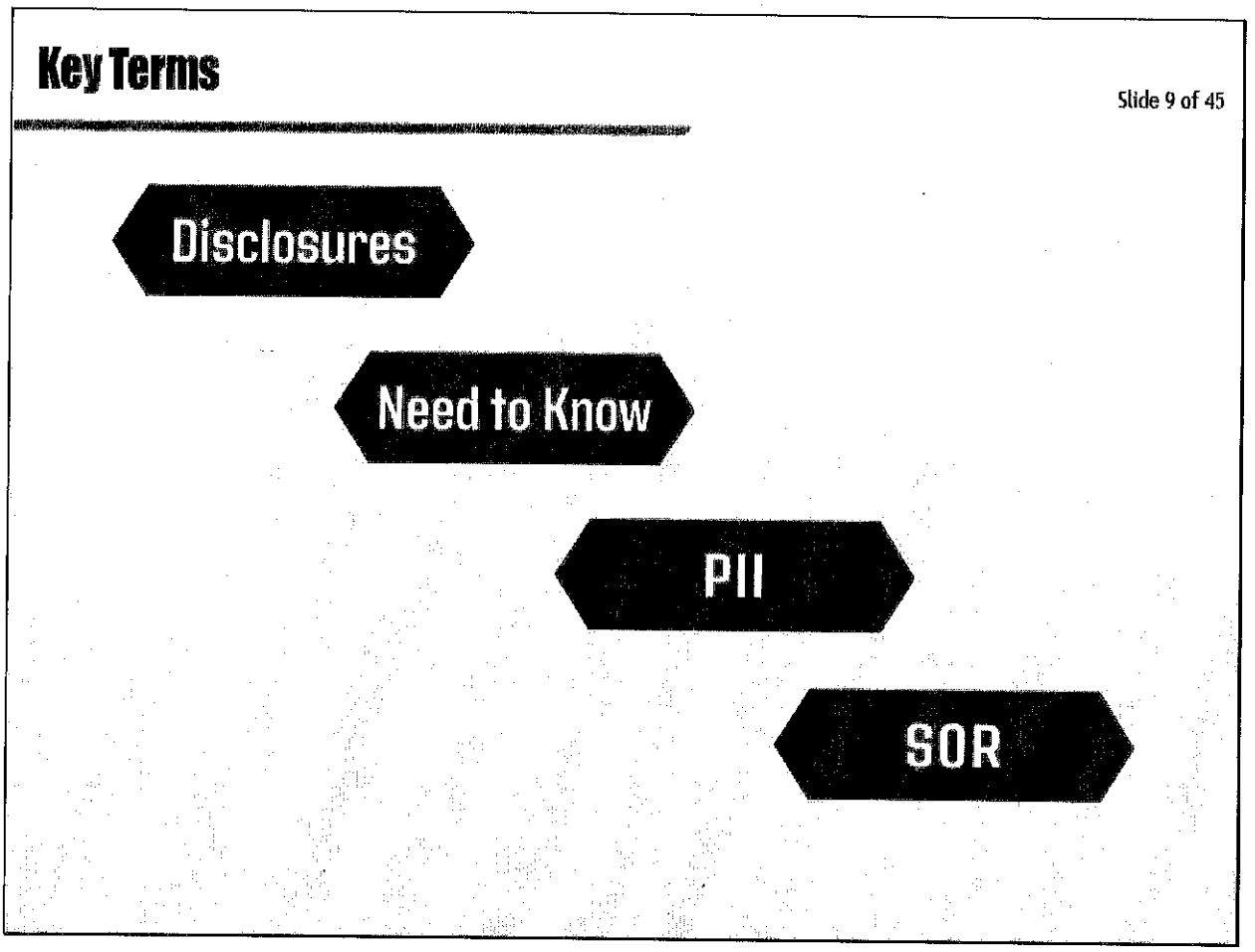
When a customer, employee, or other individual submits personal information to USPS,

we must provide a Privacy Act Statement, which includes a link to the USPS privacy policy.

This ensures the individual can make an informed decision on whether to share personal information

and informs them of USPS compliance to Privacy Act requirements.

Slide 9 - Key Terms



Slide notes

Now that you have a general idea of what the Privacy Act means to you as a USPS employee,

let's review a few key terms that will be used throughout the course.

Slide 10 - Disclosures

Disclosures

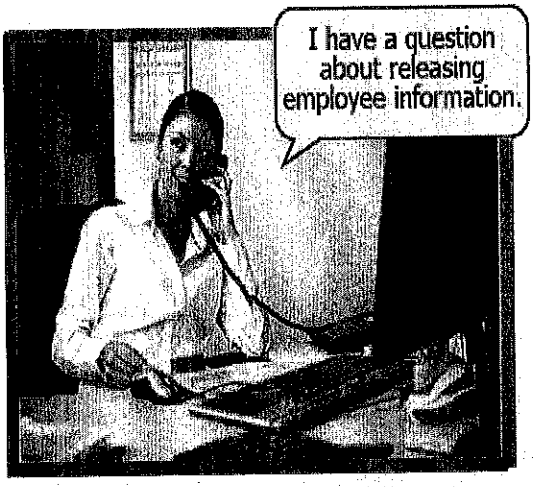
Slide 10 of 45

Definition:

- The release of personal information:
  - Internally - within USPS
  - Externally - to third parties

General rule:

- USPS will only disclose a protected record:
  - With written consent from individual to whom the record pertains.
  - When authorized to do so under the Privacy Act.



Contact the Privacy Office prior to disclosing personal information.

Slide notes

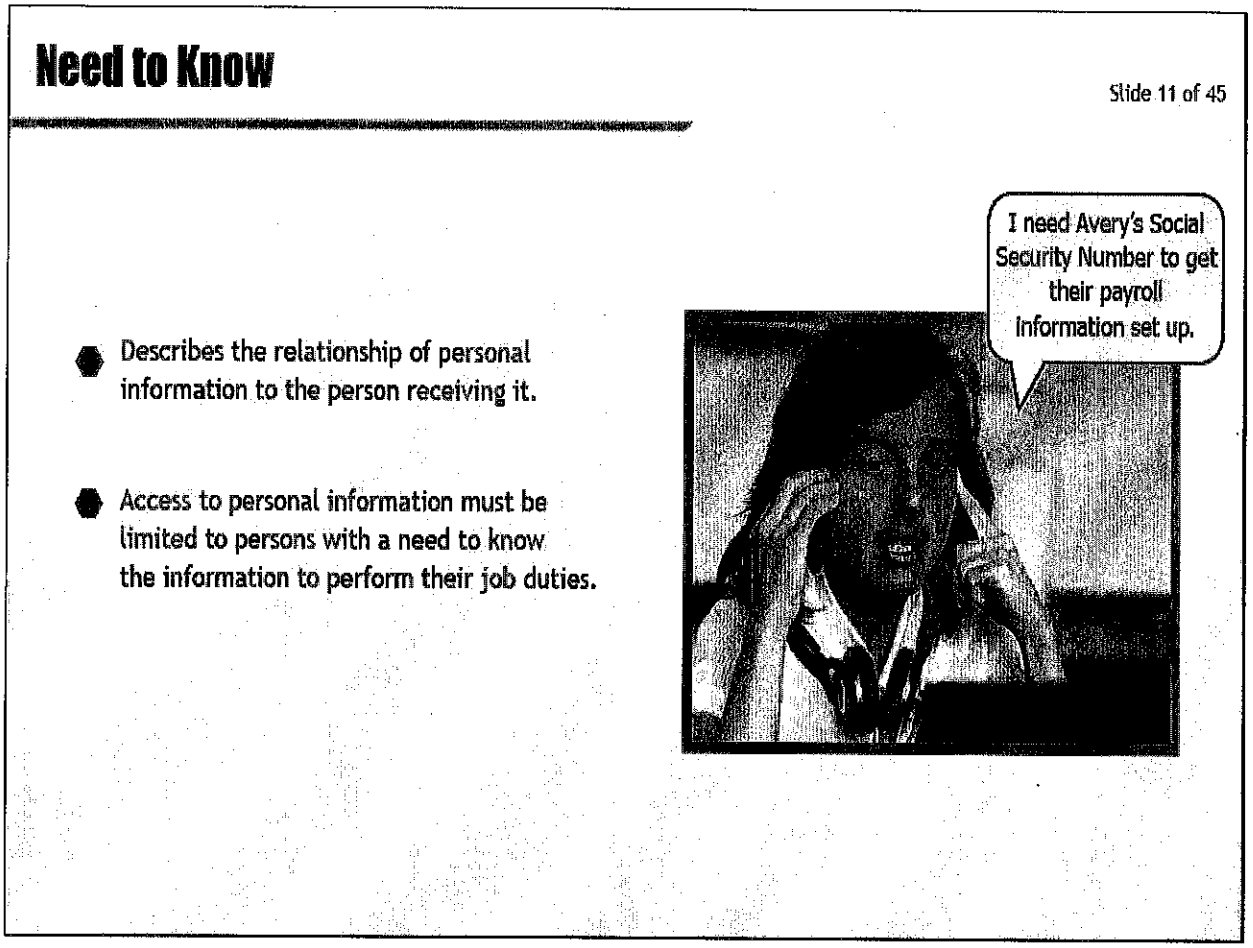
A disclosure is the release or sharing of personal information and can be made internally or externally, if authorized.

The general rule is that USPS will only disclose a record with written consent from the individual

or when authorized to do so under the Privacy Act.

Before making a decision about what information may be disclosed, consult the Privacy Office or Law Department.

Slide 11 - Need to Know



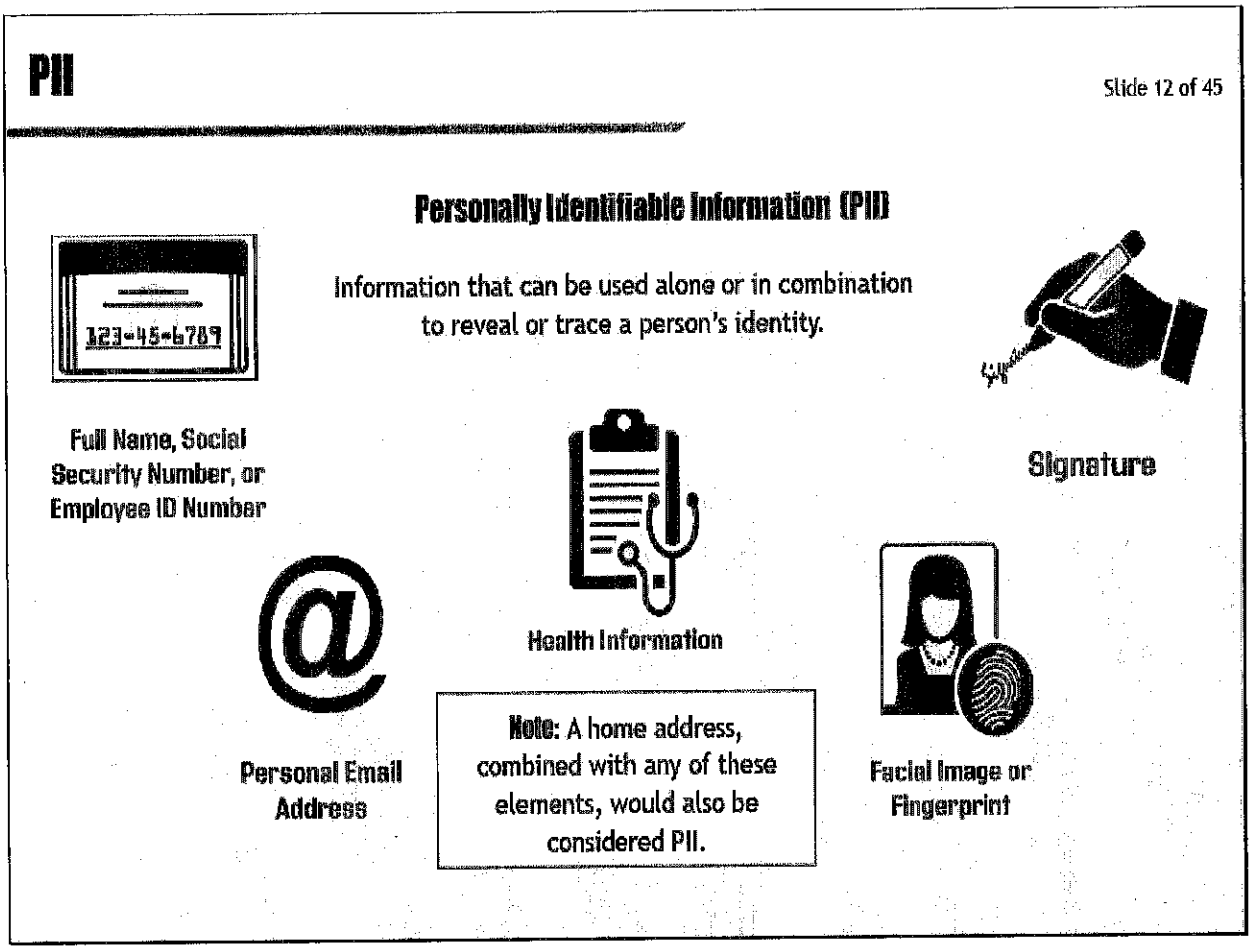
Slide notes

Need to know describes the relationship between information and the person receiving it.

Access to personal information must be limited to persons with a need to know the information to perform their job duties.

For example, an employee entering payroll information has a need to know the personal information of employees within their office, but not the information for employees in a different office.

Slide 12 - PII



Slide notes

Personally Identifiable Information, or PII, is any information that can be used alone or in combination to reveal or trace a person's identity.

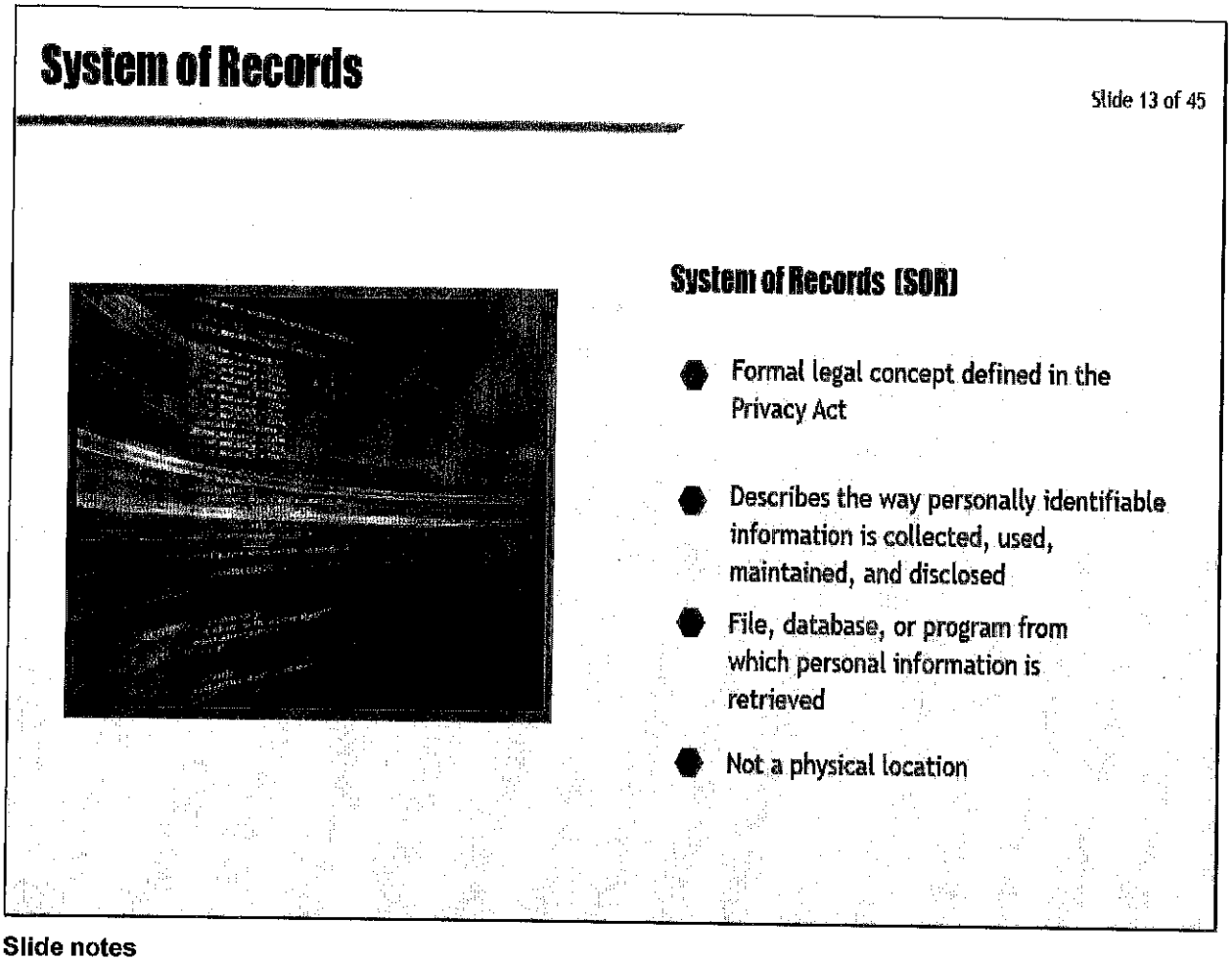
Examples of recognizable PII include a person's full name, Social Security Number, Employee Identification Number, or EIN,

personal email address, individually identifiable health information, a facial image, fingerprints, and an individual's signature.

While a home address alone is not PII, when it's combined with other identifying information,

such as a name, the address and name combined becomes PII.

Slide 13 - System of Records



Slide notes

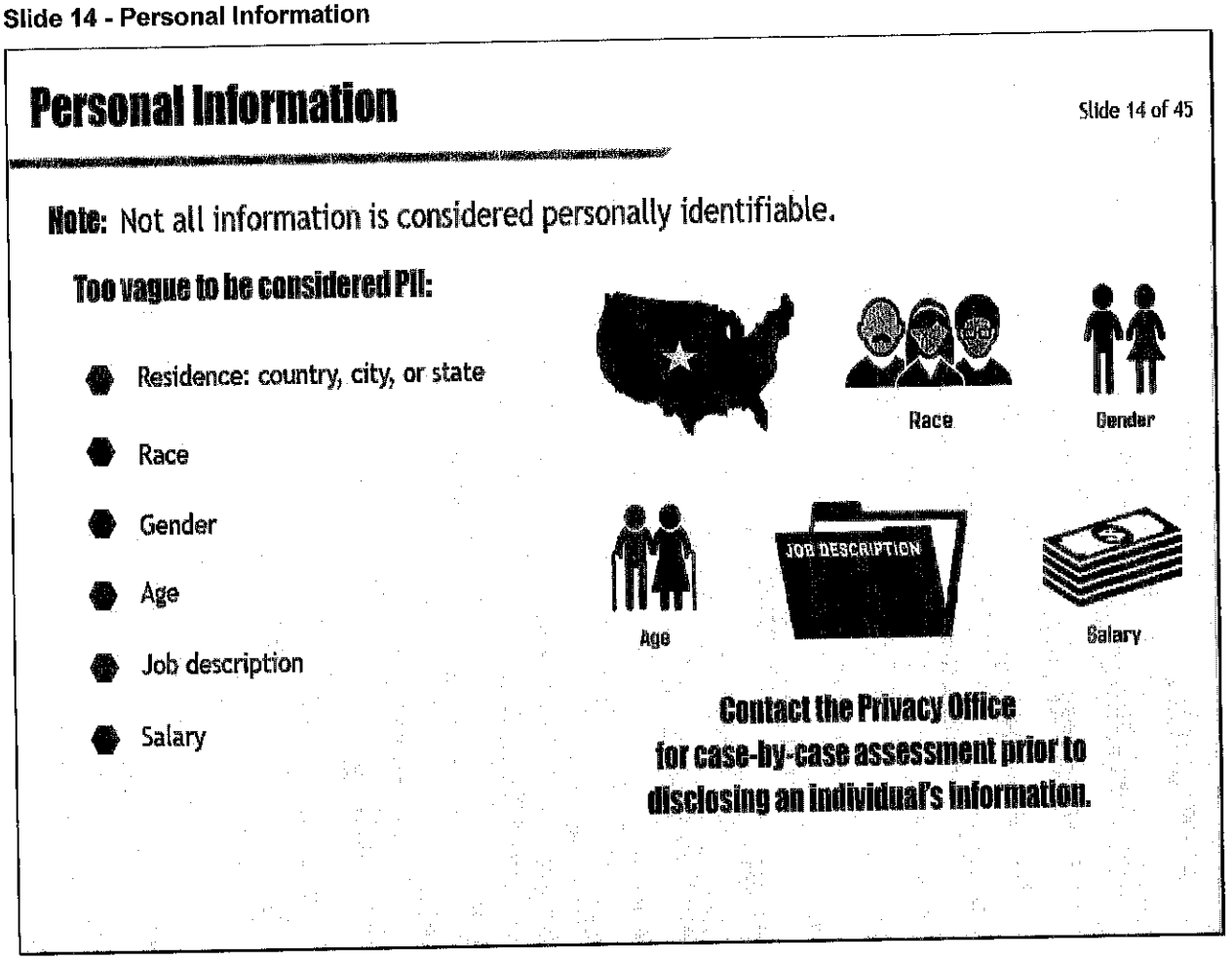
A System of Records, or SOR, is a formal legal concept defined in the Privacy Act

that describes the way personally identifiable information is collected, used, maintained, and disclosed.

A Privacy Act System of Records is a file, database, or program from which personal information is retrieved

and not a physical location, such as a server or file cabinet.

Slide 14 - Personal Information



Slide notes

It's important to note, not all information pertaining to an individual is considered personally identifiable.

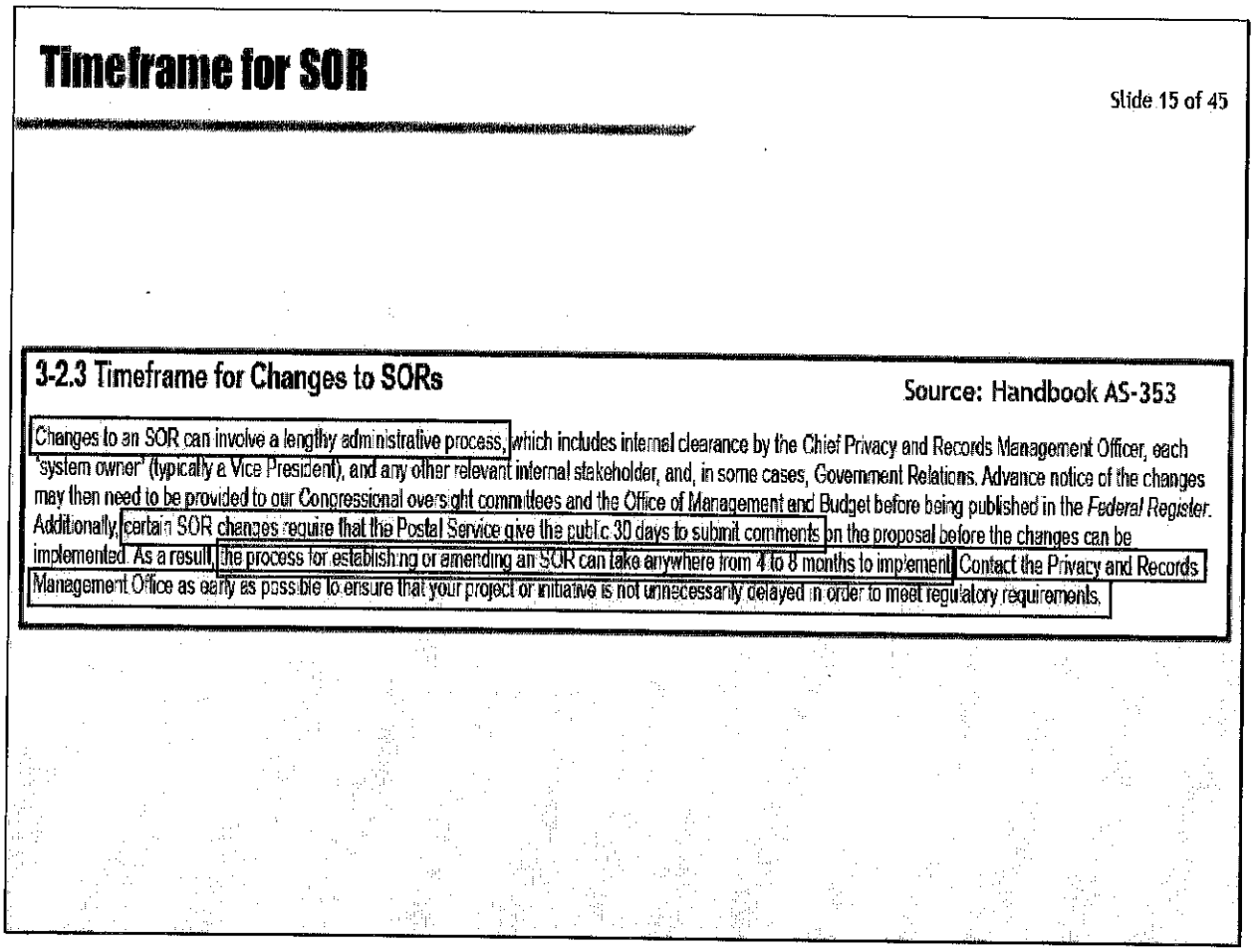
Some information is too vague to be linked to an identity. General residence information, such as a country, city,

or state would not be considered PII by itself. Additionally, referring to a race, gender, age group, job description,

or salary would not necessarily reveal someone's identity.

Whether something is PII requires a case-by-case assessment of the specific risk and should be determined by the Privacy Office.

Slide 15 - Timeframe for SOR



Slide notes

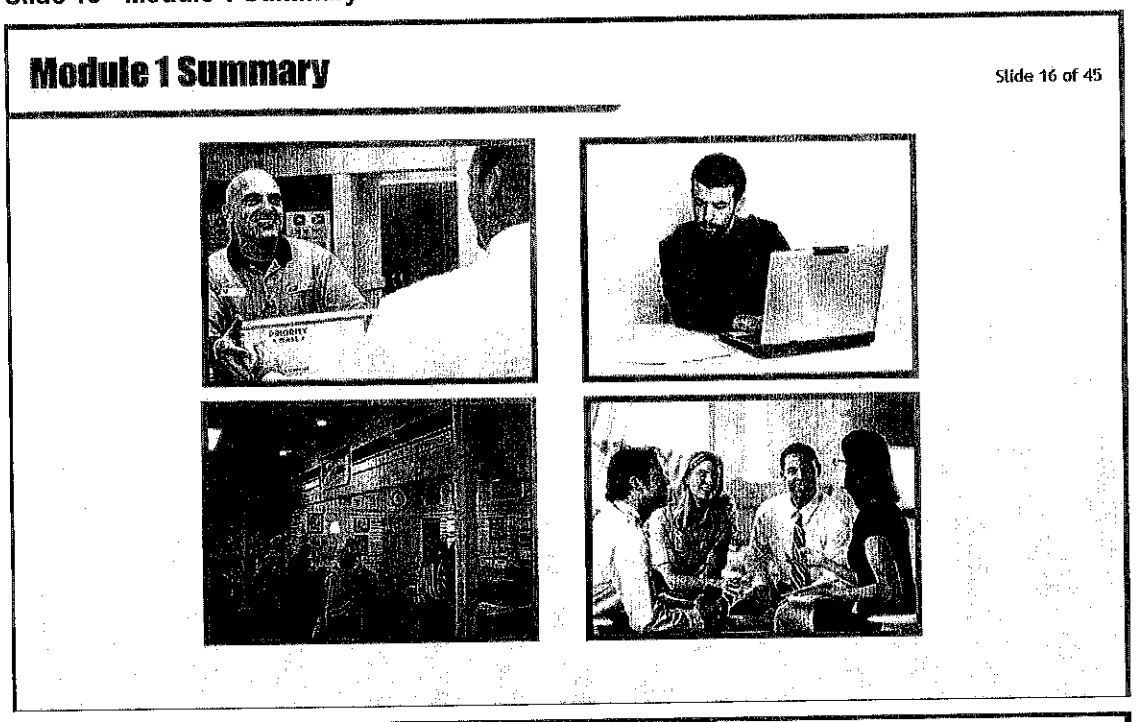
You learned the definition of an SOR, but it's important that you understand the timeframe associated with changes.

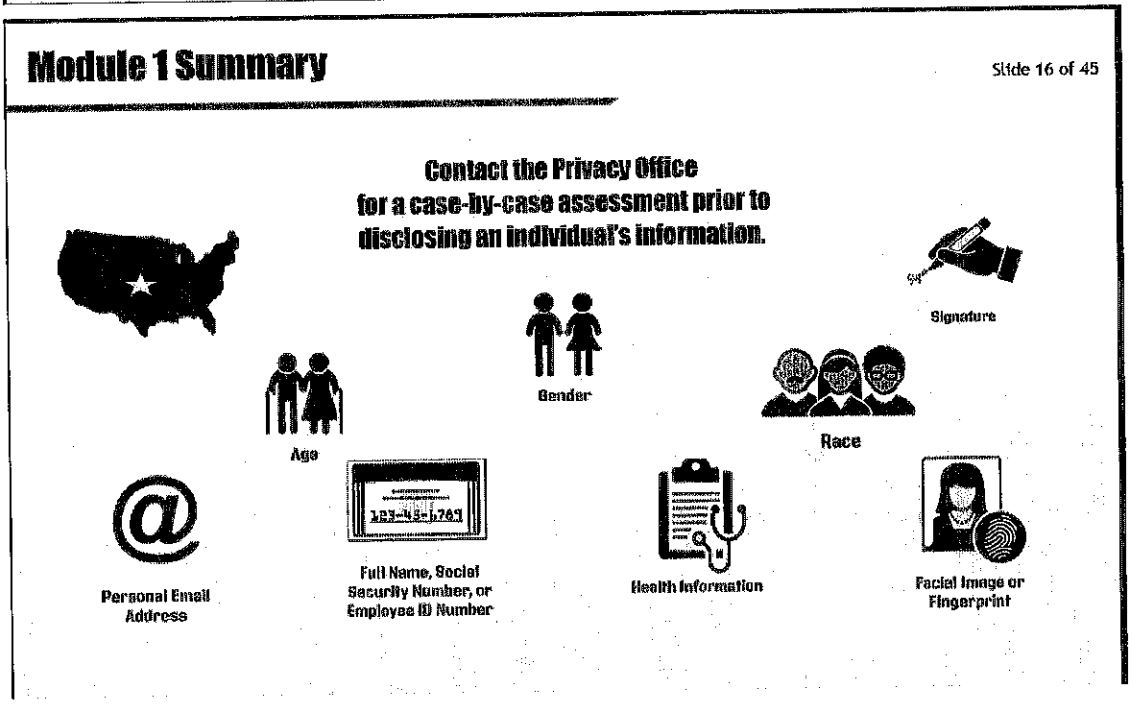
The creation or revision of an SOR is a multi-step process with mandatory time allotments for each item,

including a 30-day public comment period. You can expect the process to take 4 to 8 months to implement.

Make sure to contact the Privacy Office very early in the planning phase of any project that requires the collection of PII.

Slide 16 - Module 1 Summary





Slide notes

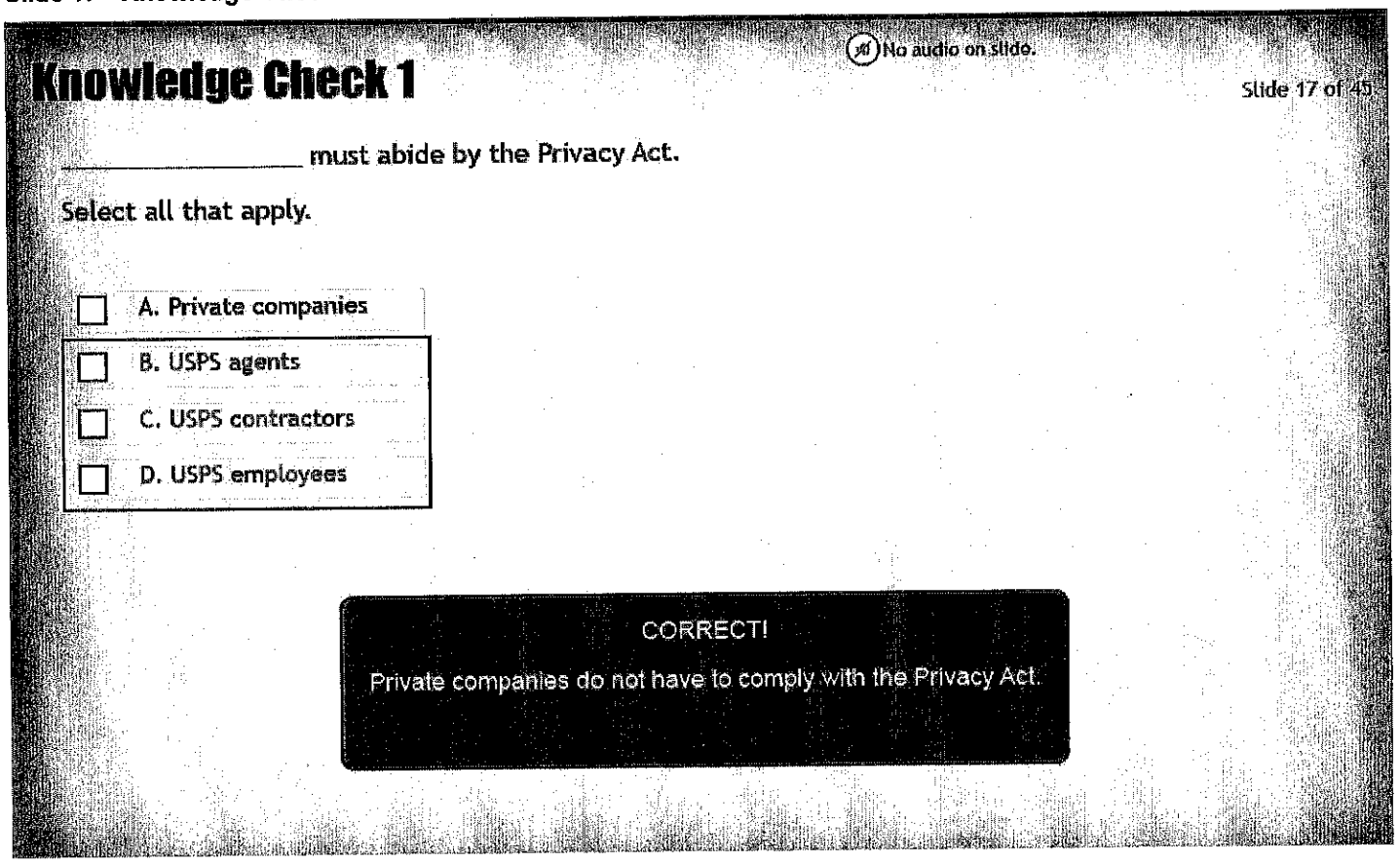
To review, USPS employees, agents, suppliers, and contractors are subject to privacy protection requirements of the Privacy Act.

Since it's often difficult to understand when information should be considered PII,

and because violations of the Privacy Act can lead to disciplinary action, up to and including termination,

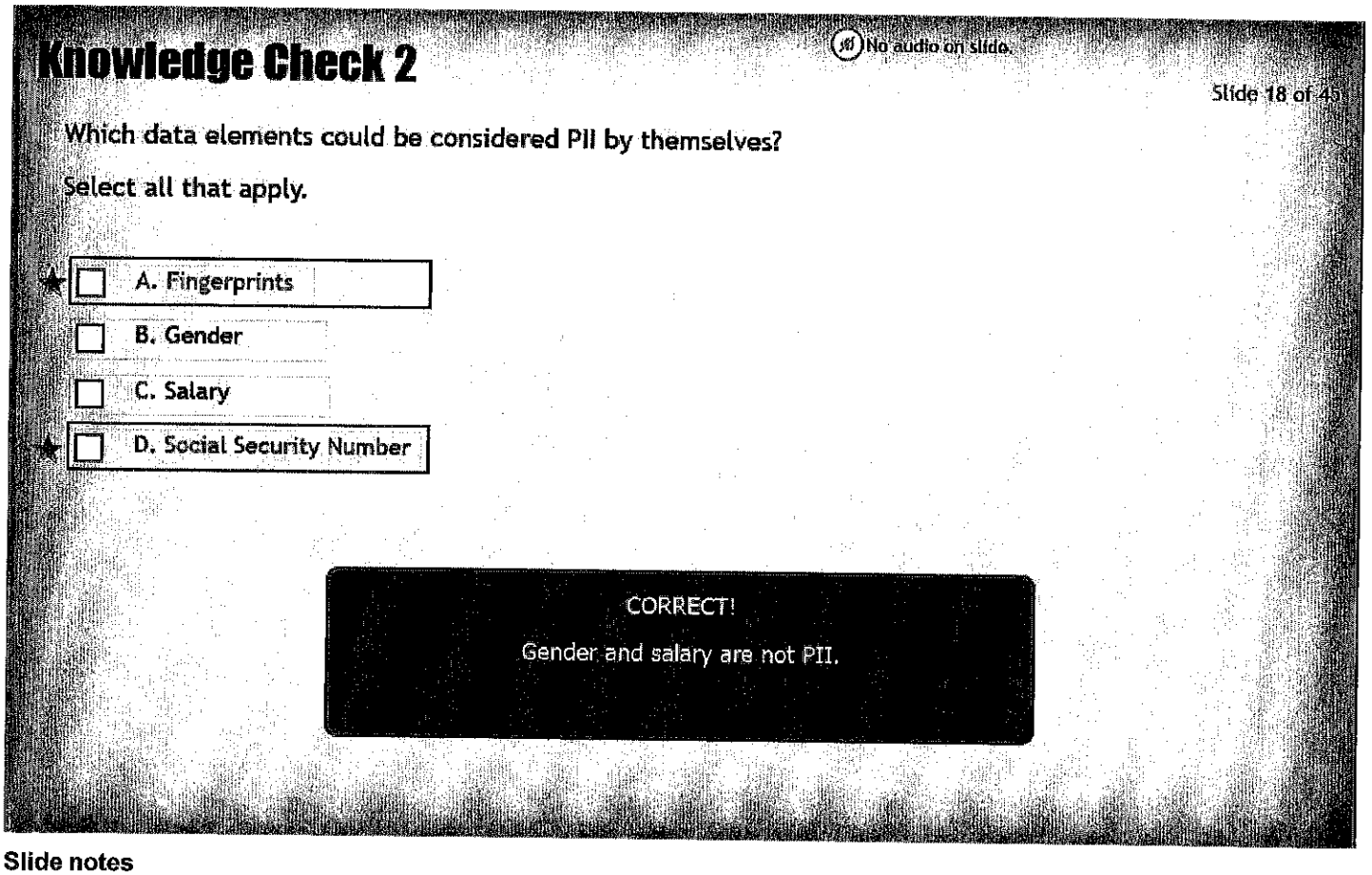
always remember to contact the Privacy Office for guidance before disclosing another individual's information.

Slide 17 - Knowledge Check 1



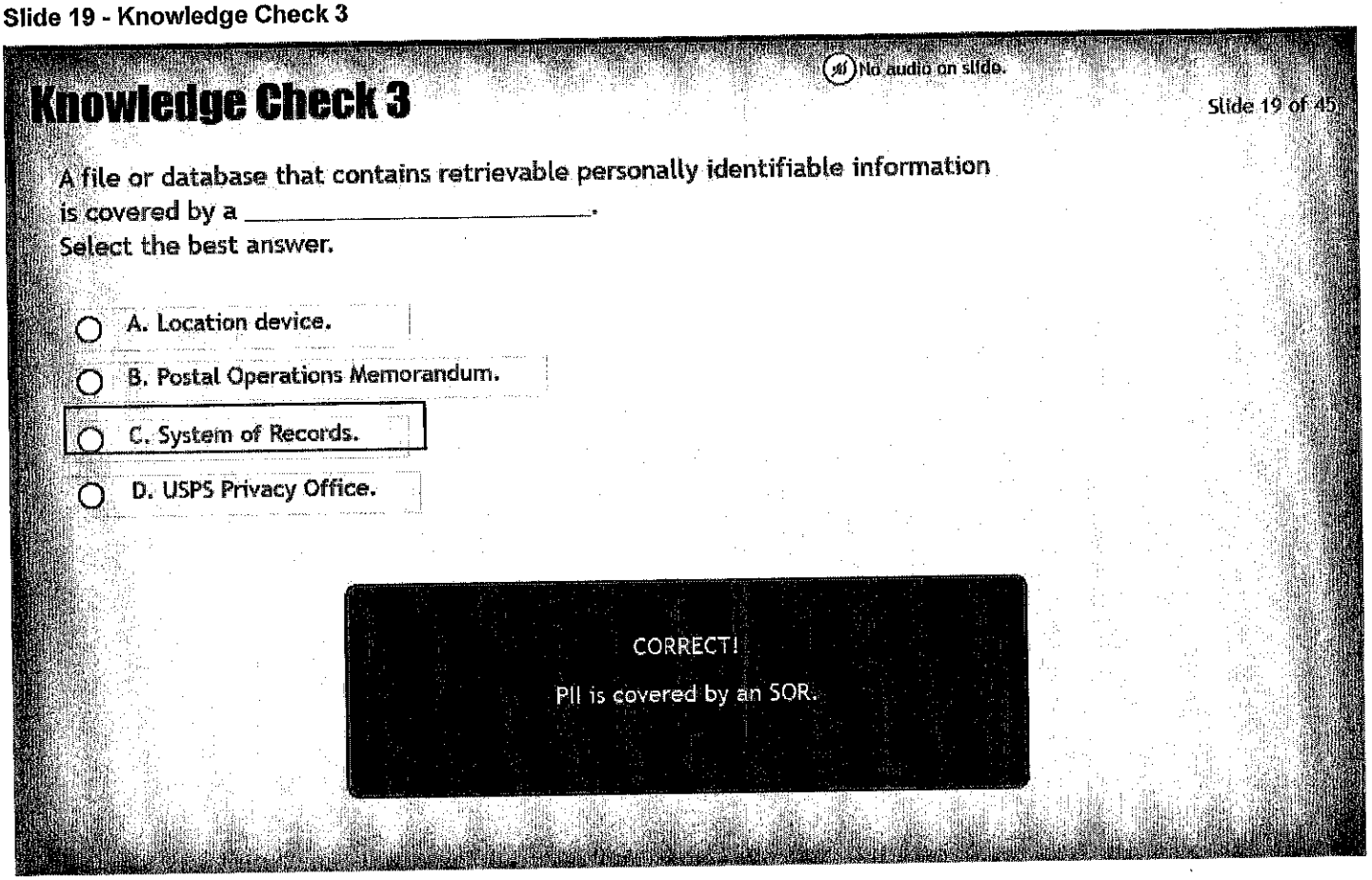
Slide notes

Slide 18 - Knowledge Check 2



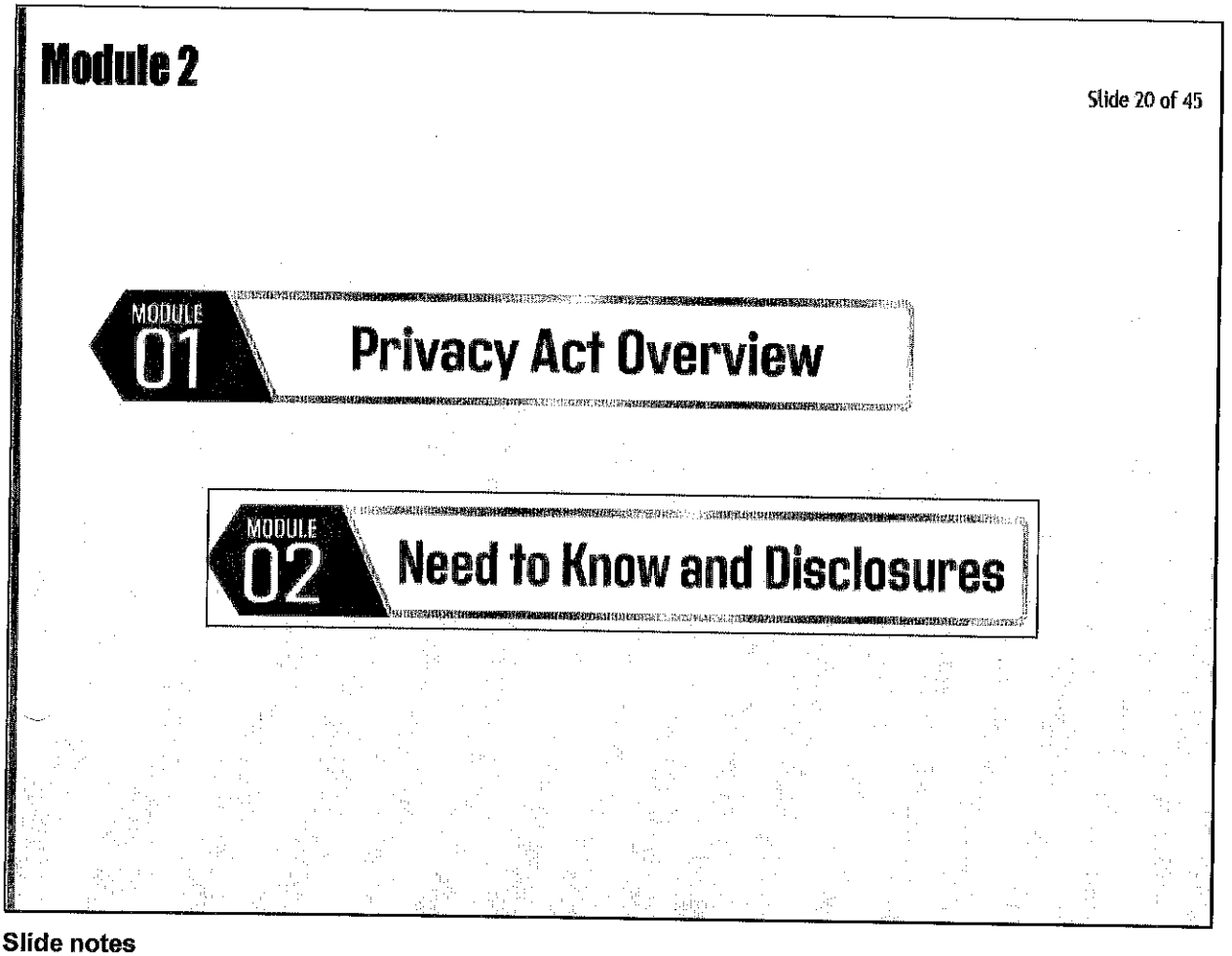
Slide notes

Slide 19 - Knowledge Check 3



Slide notes

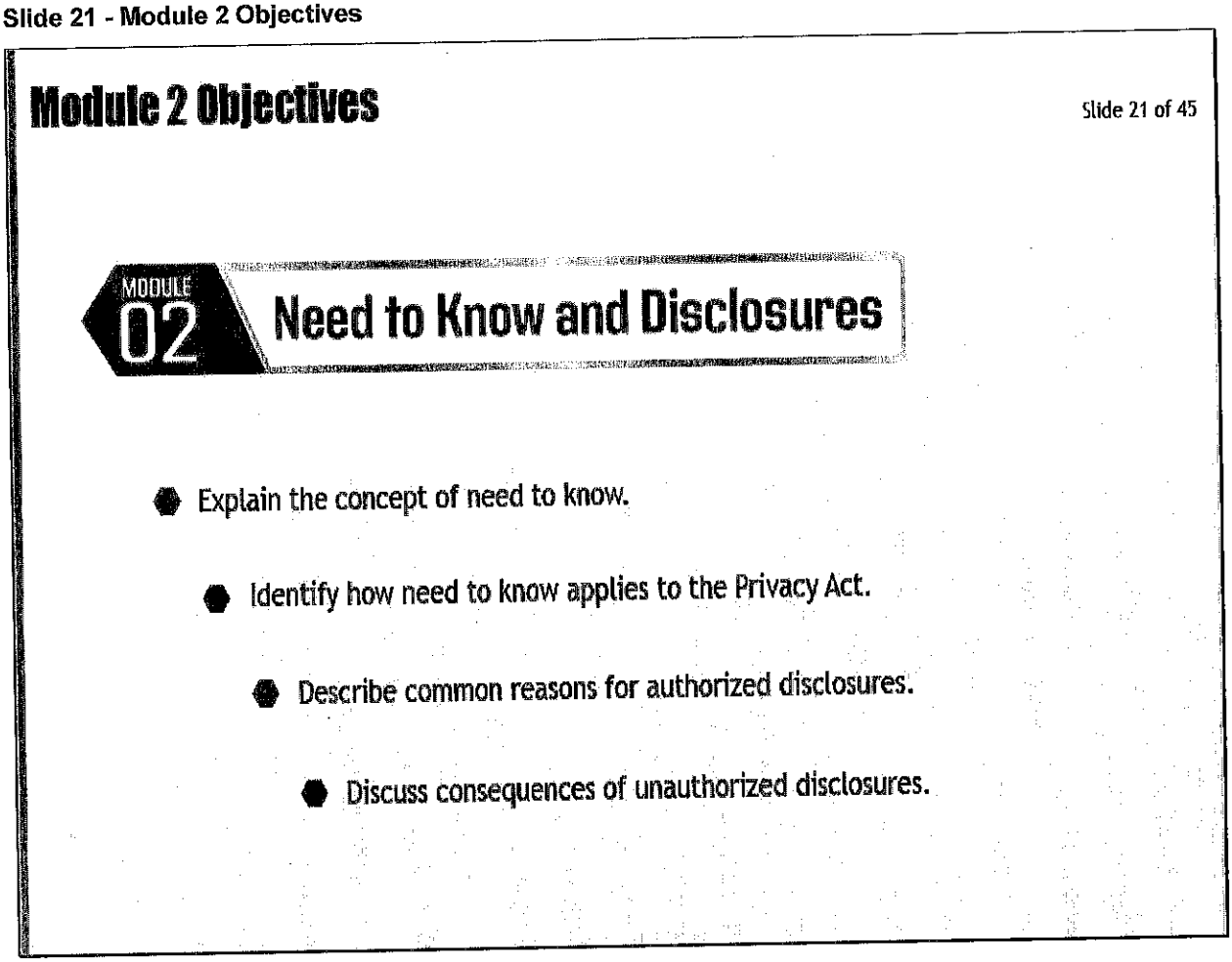
Slide 20 - Module 2



Slide notes

Welcome to Module 2, Need to Know and Disclosures. In this module, we'll go further in depth on the topics of need to know and disclosure.

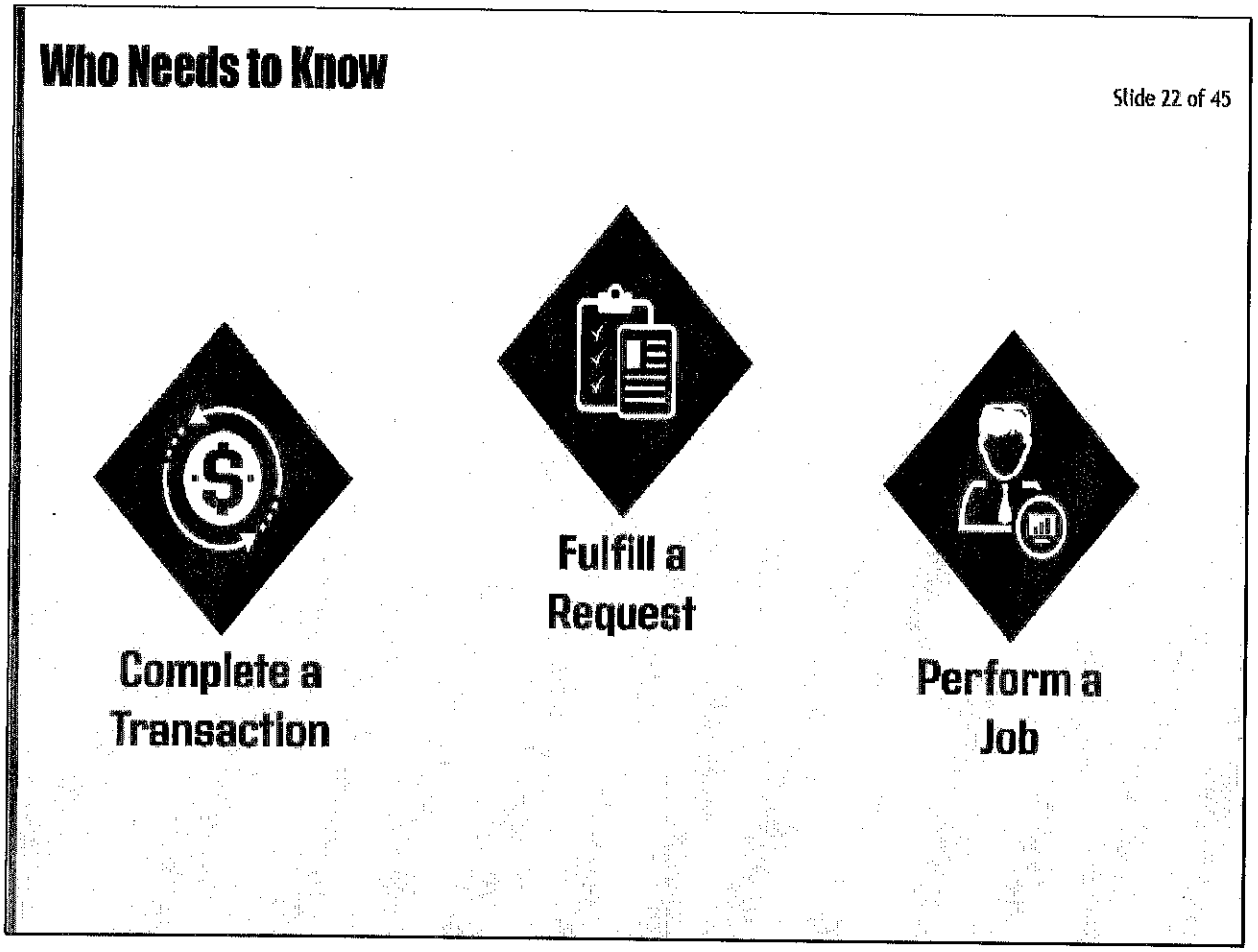
Slide 21 - Module 2 Objectives



Slide notes

By the end of this module, you should be able to explain the concept of need to know and identify how it applies to the Privacy Act, describe common reasons for authorized disclosures, and discuss consequences of unauthorized disclosures.

Slide 22 - Who Needs to Know

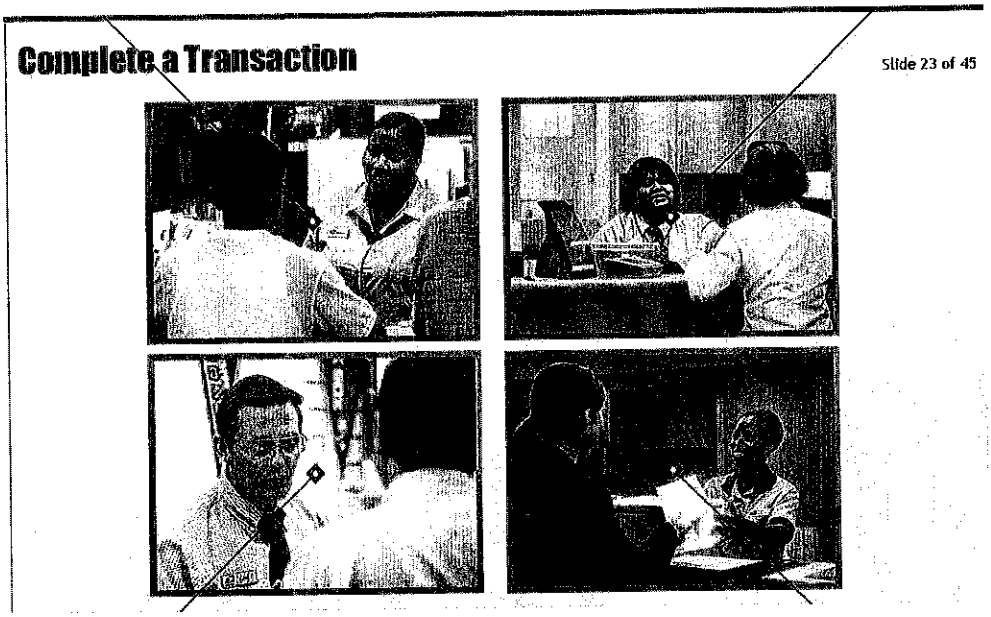


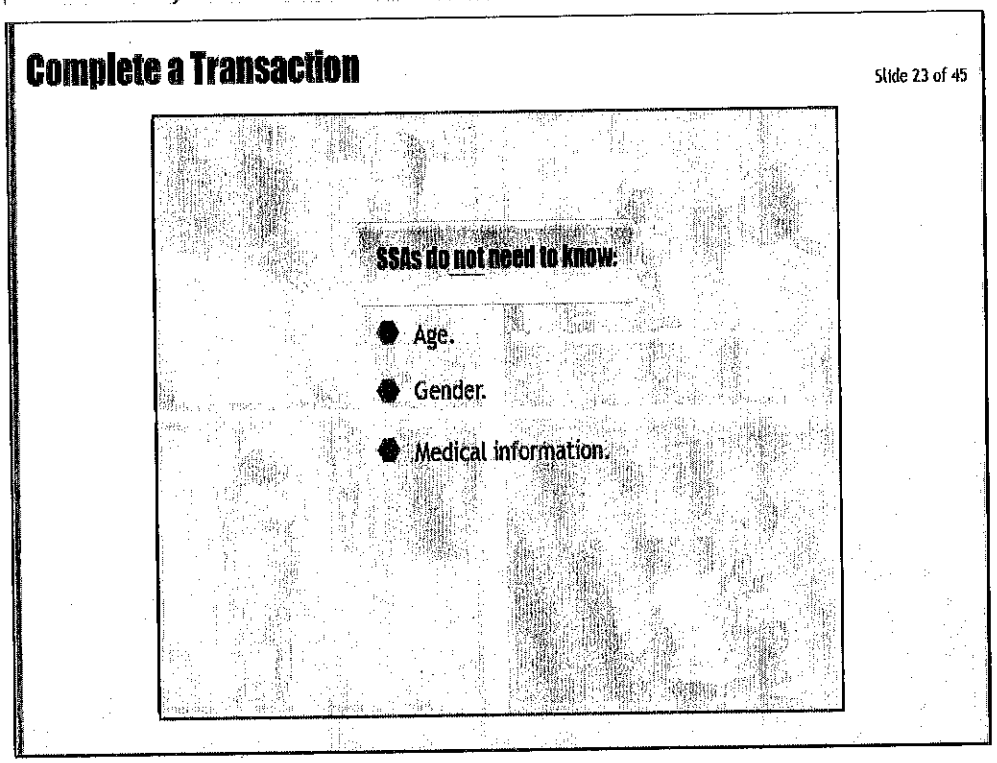
Slide notes

In the context of USPS, need to know largely pertains to internal employees and contractors

who need other individuals' personal information to complete a transaction, fulfill a request, or perform their job.

Slide 23 - Complete a Transaction





Slide notes

Sales and Services Associates (SSAs) have a need to know customers' full names, addresses, phone numbers, and email addresses in order to complete retail transactions.

SSAs do not have a need to know information such as age, gender, or medical information.

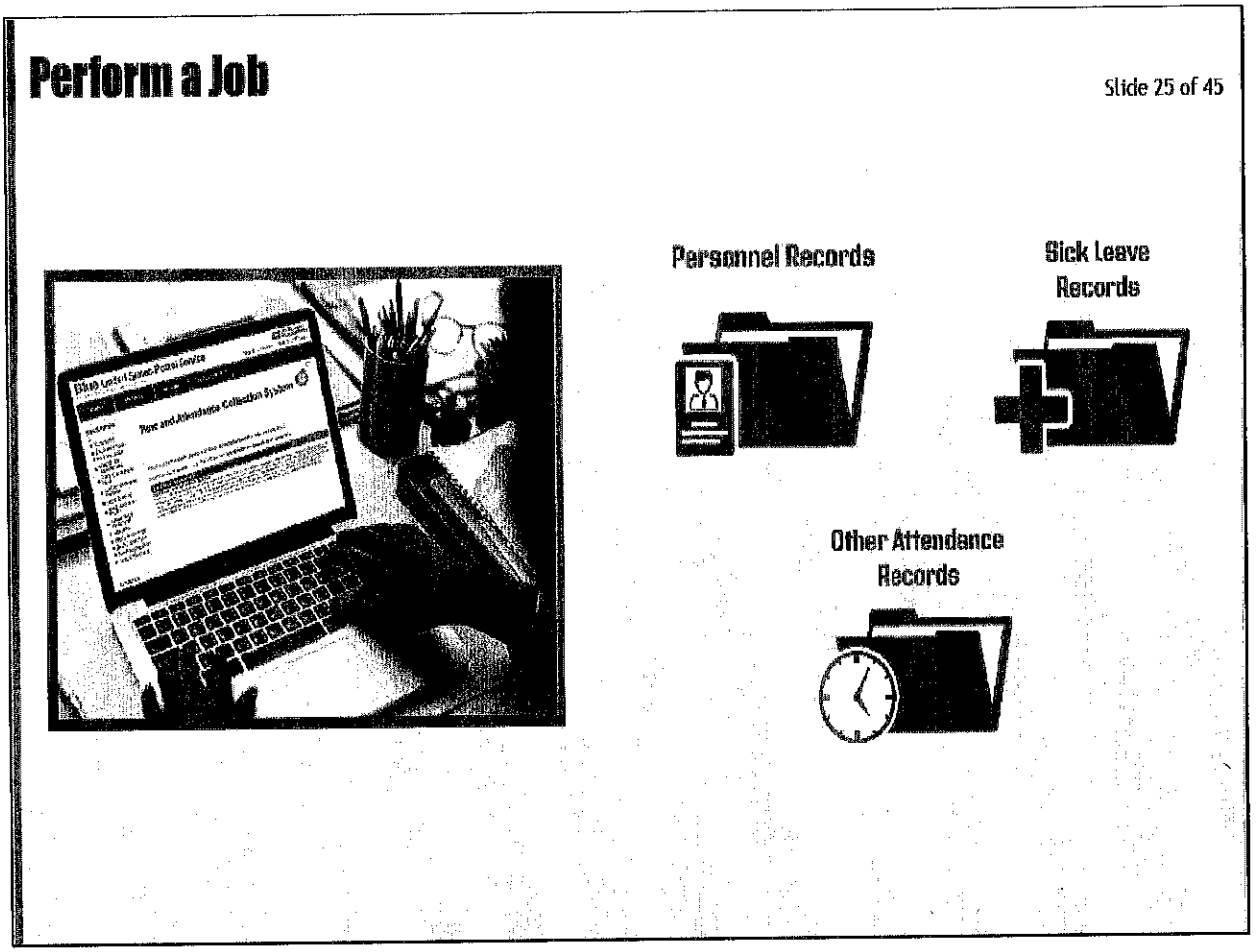
Slide 24 - Fulfill a Request

Slide notes

Should you need to call Human Resources, or HR, to inquire about benefit plans,

the HR representative would need to collect your PII so they can fulfill your request.

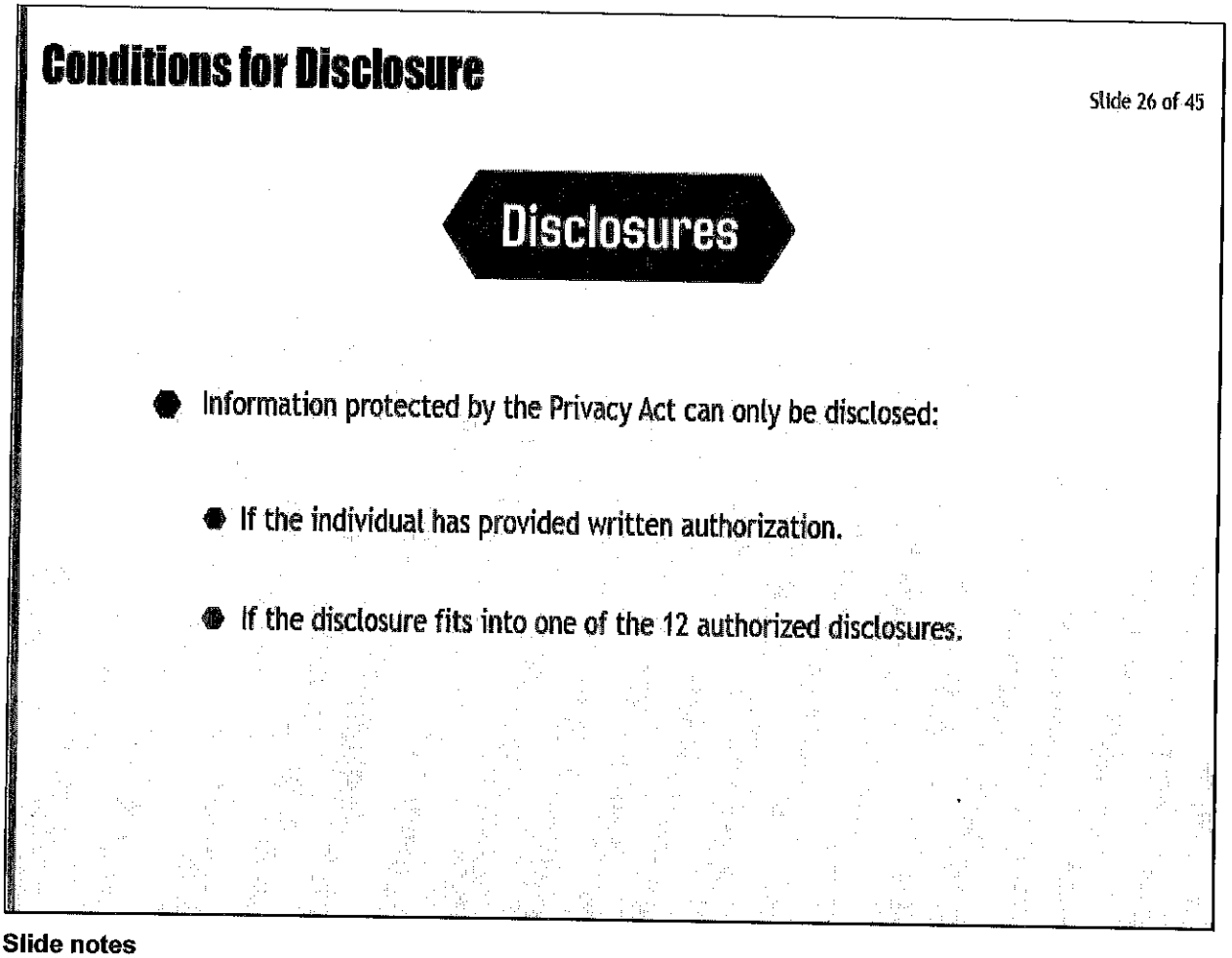
Slide 25 - Perform a Job



Slide notes

A person entering time and attendance has a need to know other employees' identification numbers, annual and sick leave balances, and what type of leave is being used.

Slide 26 - Conditions for Disclosure



Slide notes

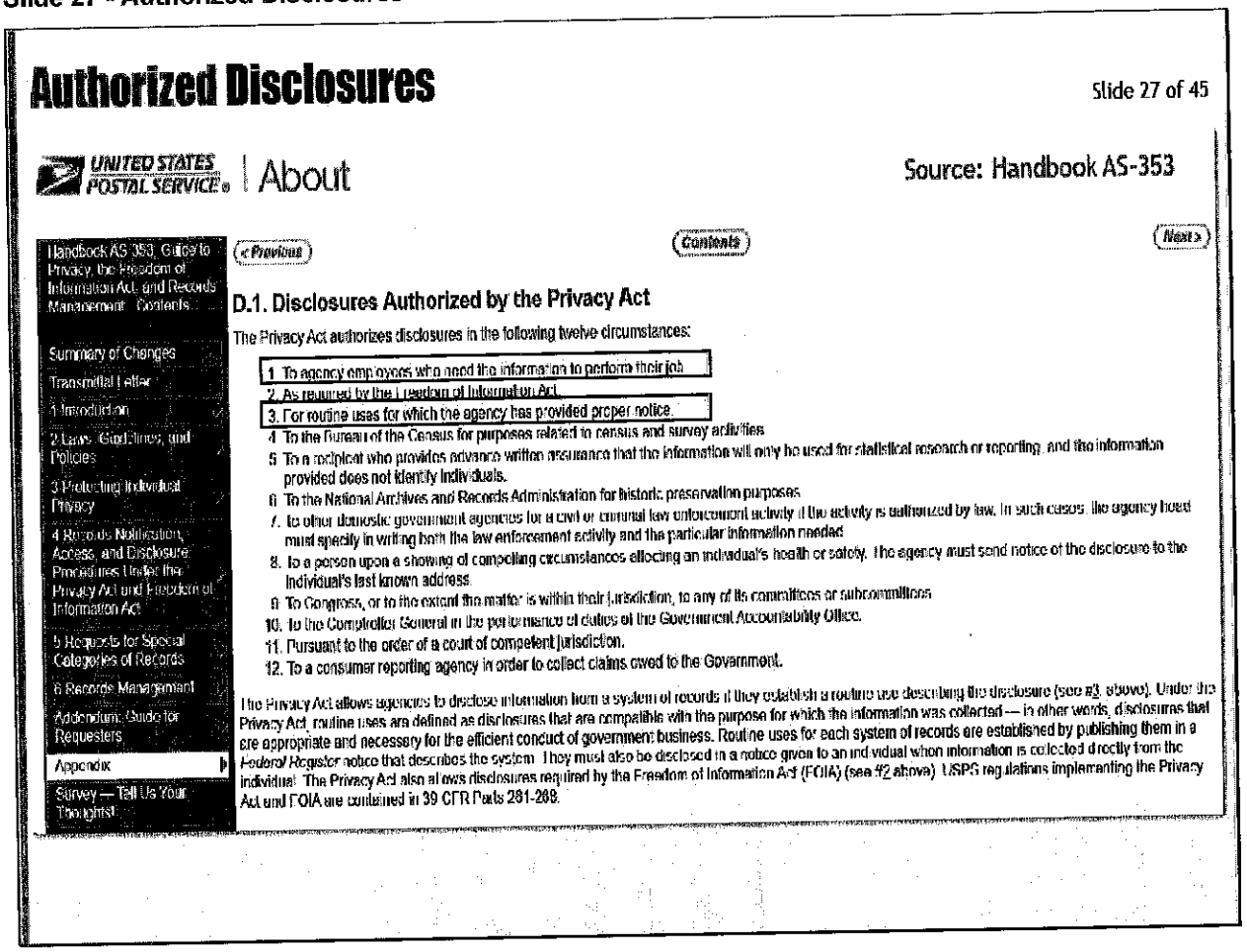
In Module 1, you learned the basic definition of a disclosure, but not specific examples of each.

Information protected by the Privacy Act can only be disclosed under two conditions:

if the individual has provided written authorization or if the disclosure fits into one of the 12 authorized disclosures under the Privacy Act.

Let's look at those.

Slide 27 - Authorized Disclosures



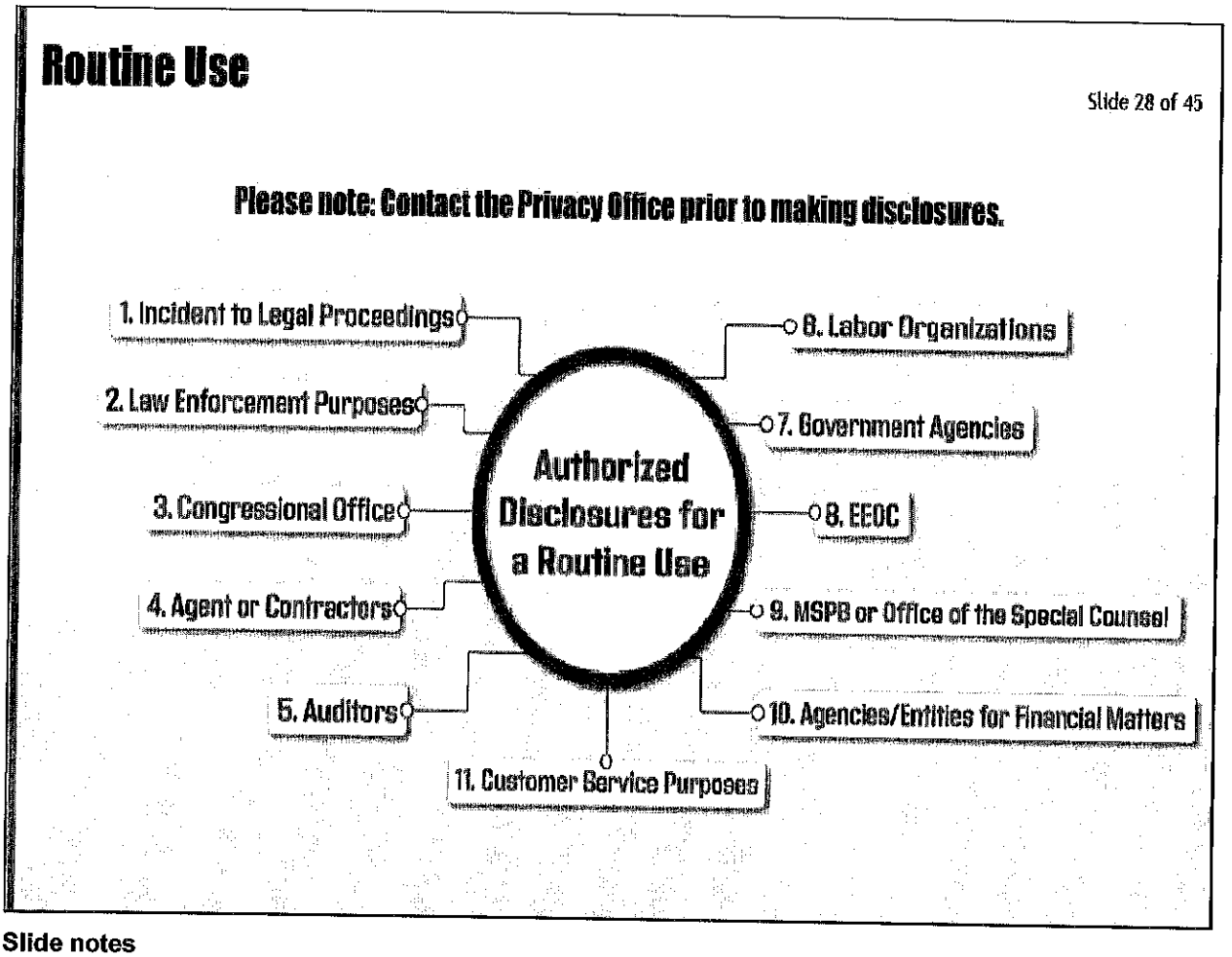
Slide notes

The Privacy Act authorizes disclosures under twelve circumstances.

Typically, the two types of authorized disclosures that will apply to you in the workplace

are the need to know to perform official job duties or under a USPS routine use.

Slide 28 - Routine Use



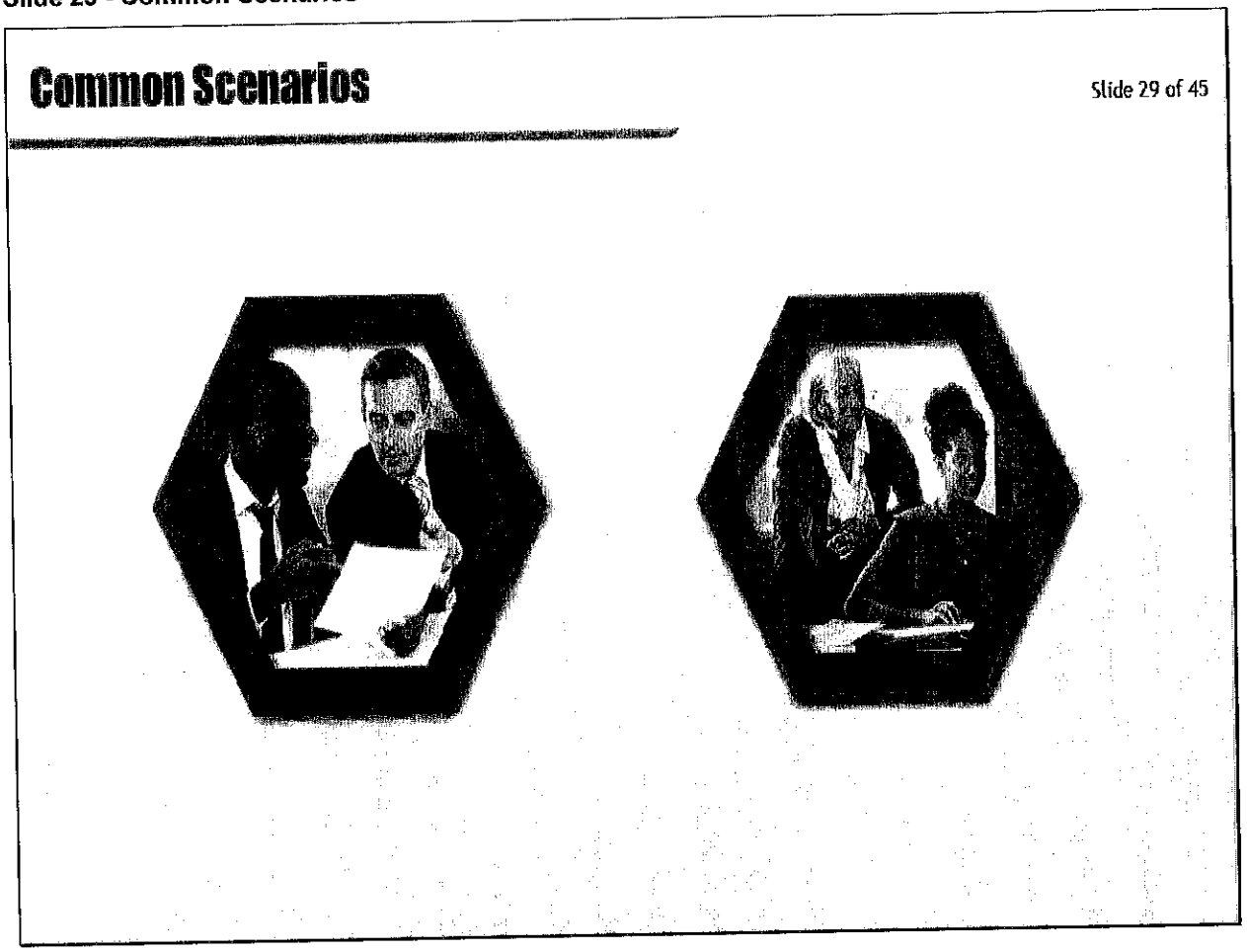
Slide notes

A routine use refers to authorized disclosures of information for recurring situations.

One example of a routine use is to provide the contractors who maintain the Informed Delivery platform with PII of USPS customers.

It is important to note, you must seek guidance from the Privacy Office to identify which records can be disclosed via a routine use.

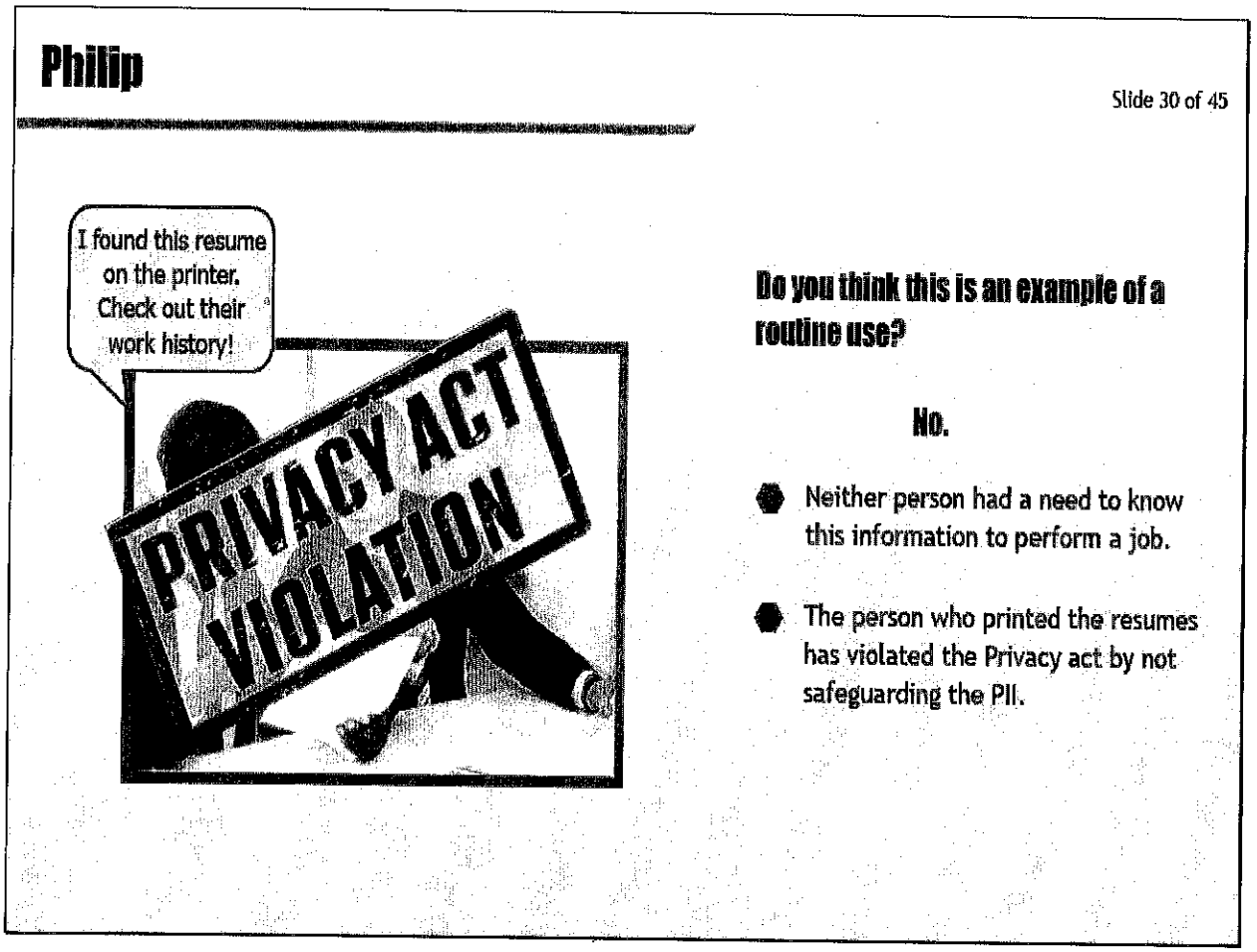
Slide 29 - Common Scenarios



Slide notes

Now, let's review two workplace scenarios involving the Privacy Act.

Slide 30 - Philip



Slide notes

Philip finds a stack of resumes on the printer, so he skims through a couple of them,

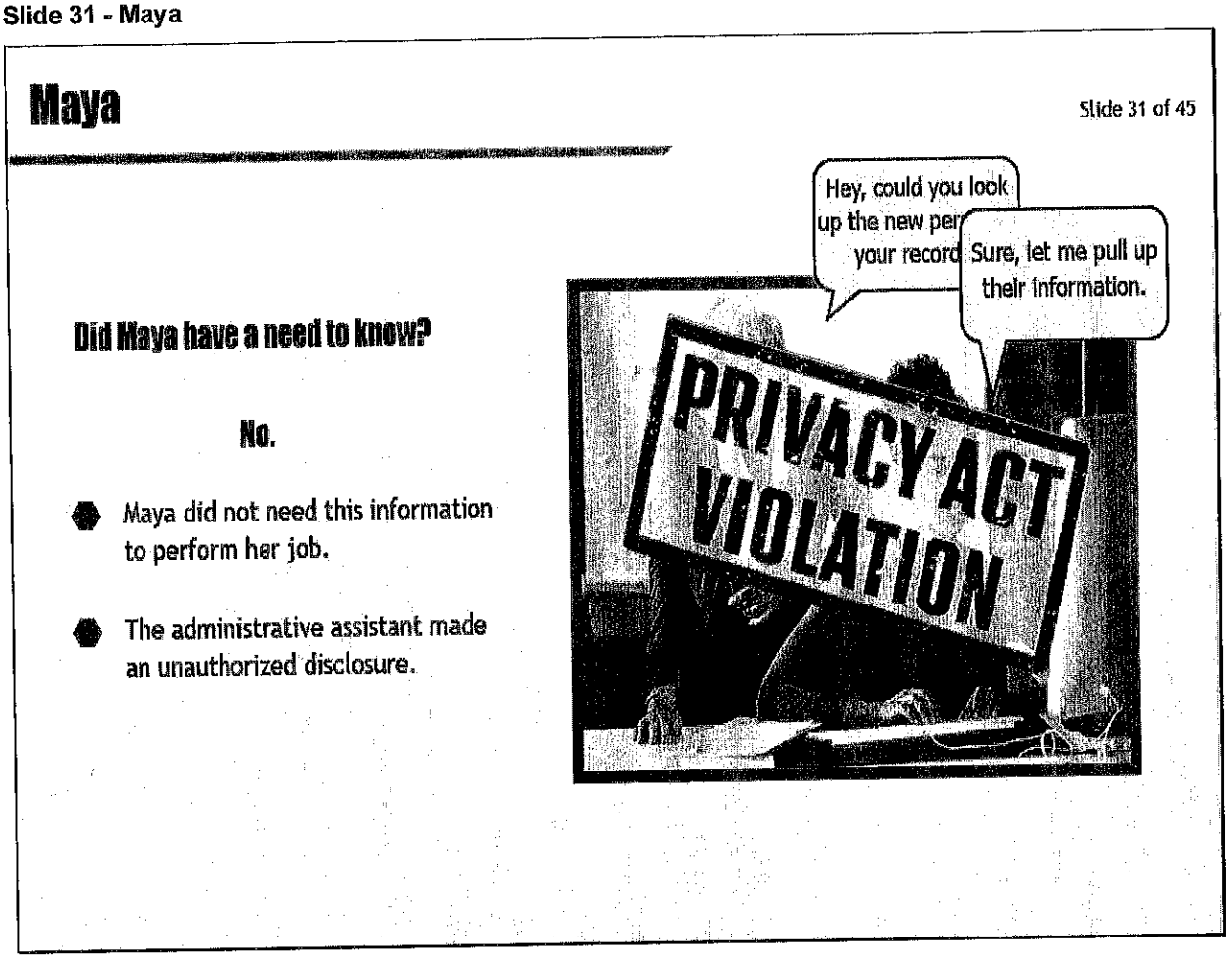
then he shares one of the resumes with a coworker.

Do you think this is an example of a routine use?

No. Neither of these gentlemen had a need to know this information,

and whomever printed the resumes has violated the Privacy Act by not safeguarding the PII.

Slide 31 - Maya



Slide notes

Maya is curious about a new employee, so she asks her friend, an administrative assistant, to look at their personnel record.

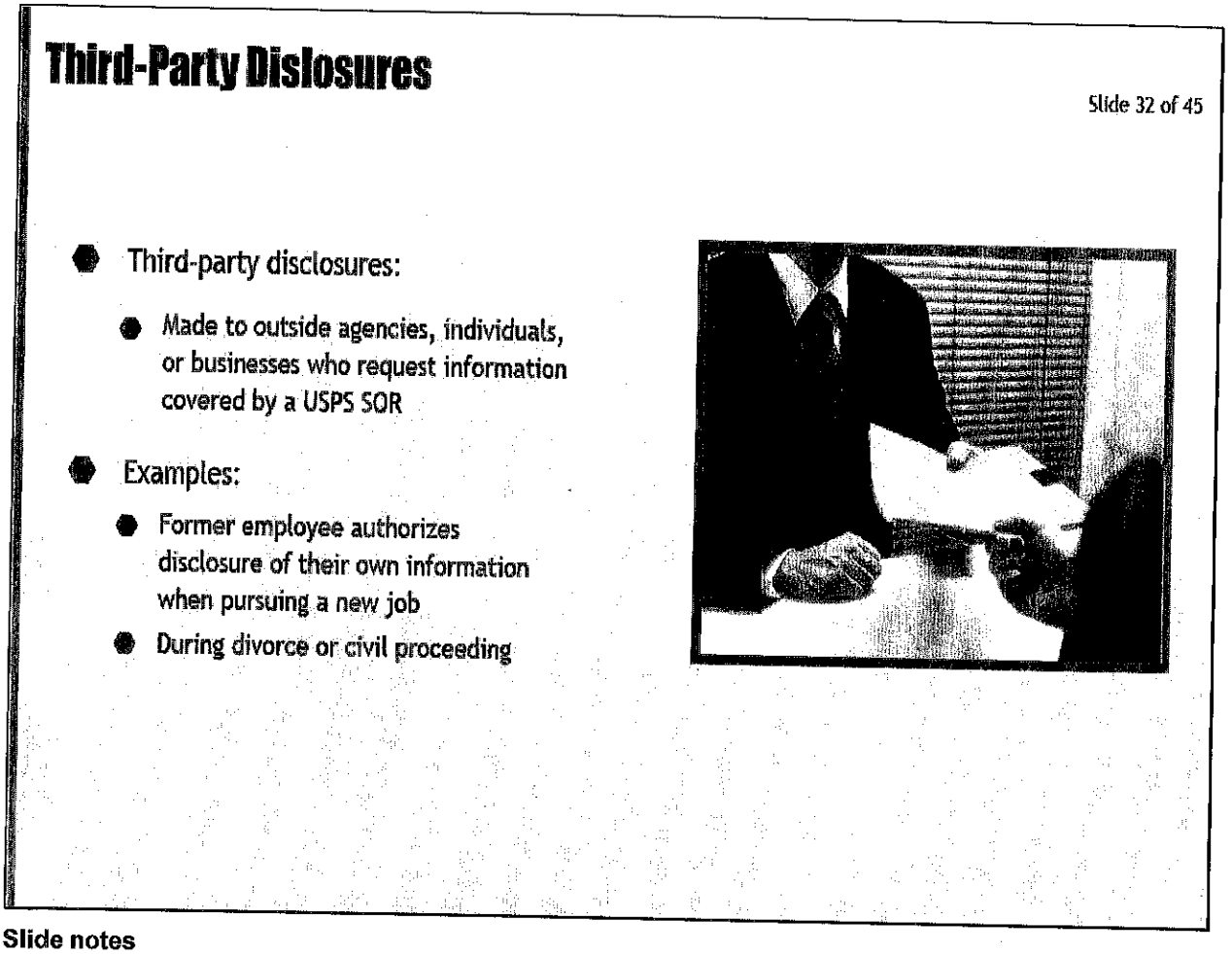
Her friend doesn't see any harm and provides Maya with a name, home address, and personal cell phone number.

Do you think Maya had a need to know?

No. Maya did not need to know this information to perform her job,

and the administrative assistant made an unauthorized disclosure.

Slide 32 - Third-Party Disclosures



Slide notes

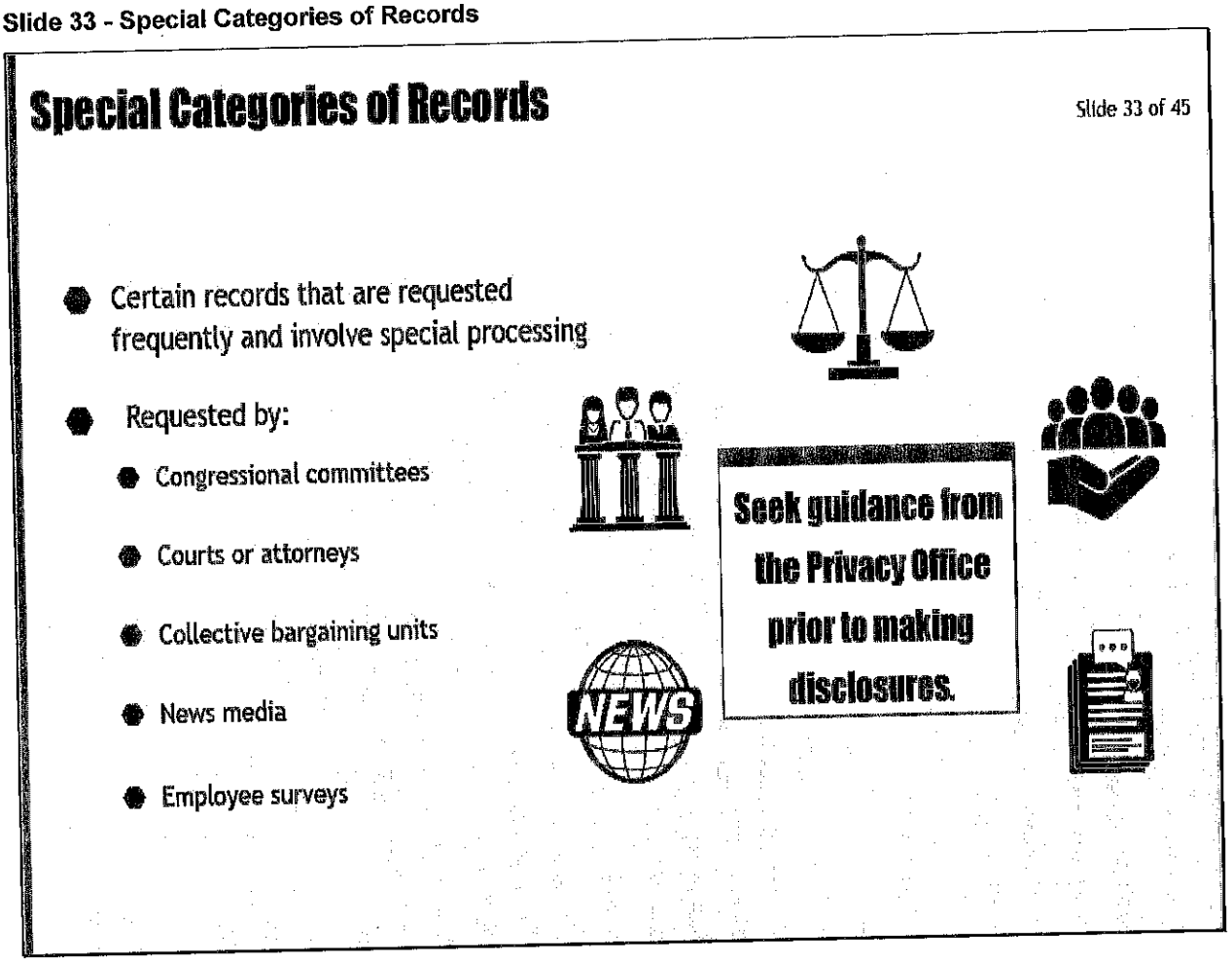
Third-party disclosures are made to outside agencies, individuals,

or businesses who request information covered by a USPS Privacy Act System of Records.

Two common scenarios of this are when a former employee authorizes the disclosure of their own information for a job search

or during a divorce or civil proceeding.

Slide 33 - Special Categories of Records



Slide notes

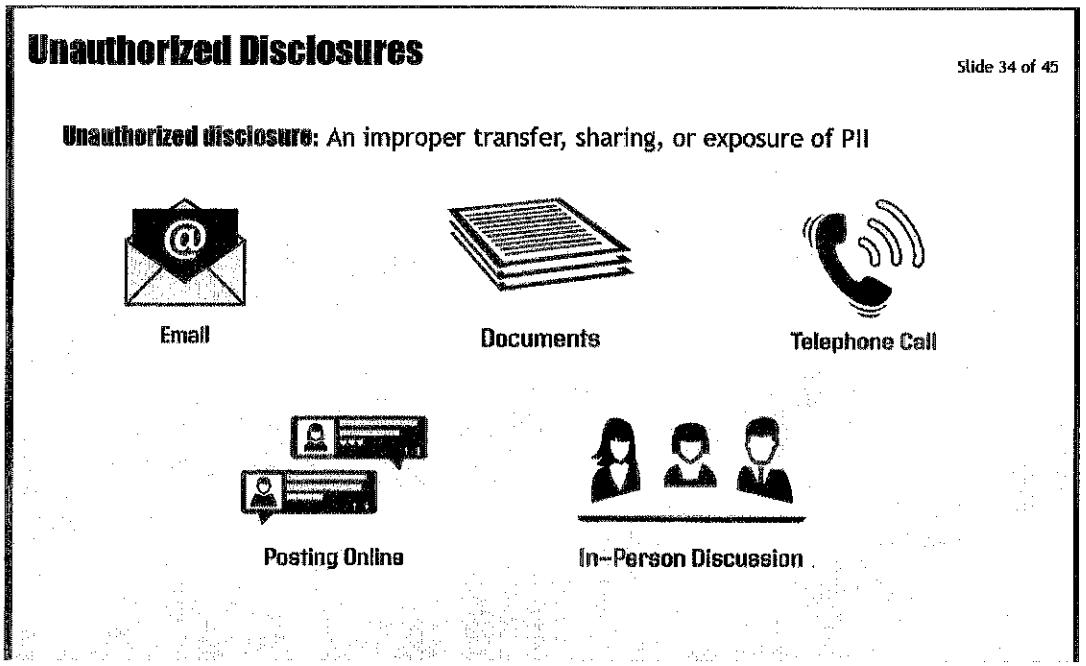
Certain categories of records within an SOR may be requested frequently and involve special processing.

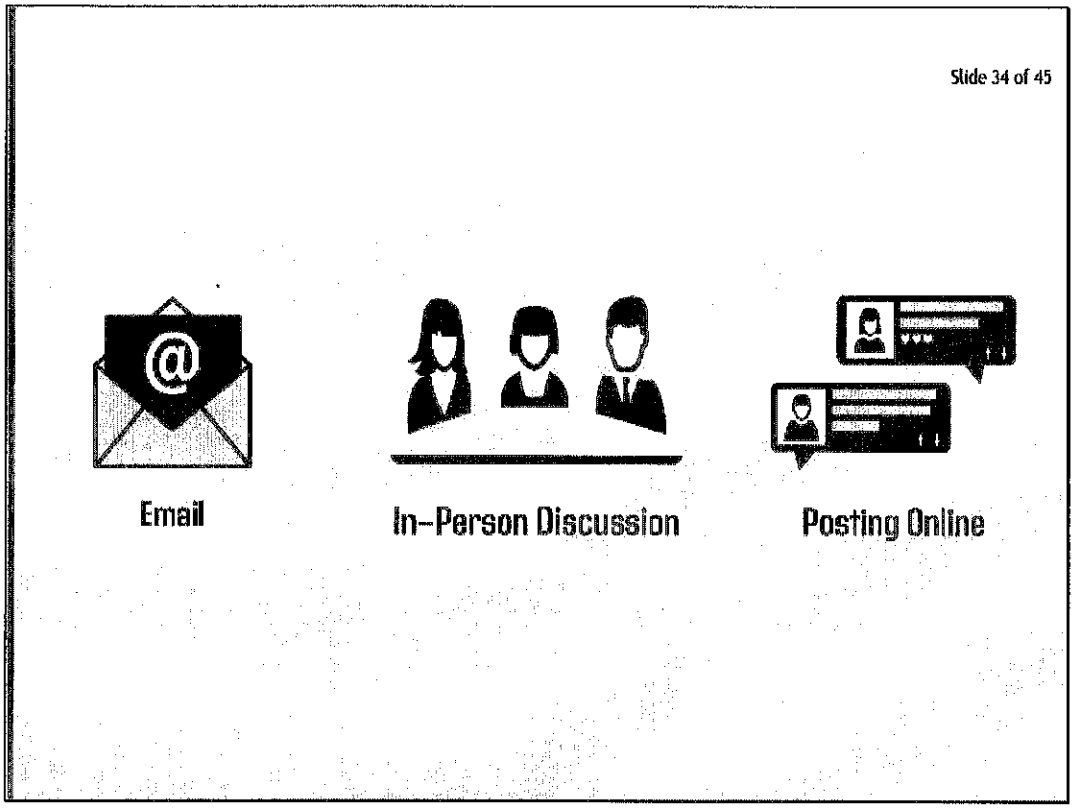
These include requests from Congressional committees, courts or attorneys, collective bargaining units,

the news media, or for employee surveys.

Again, seek direction and guidance from the Privacy Office prior to disclosing records.

Slide 34 - Unauthorized Disclosures





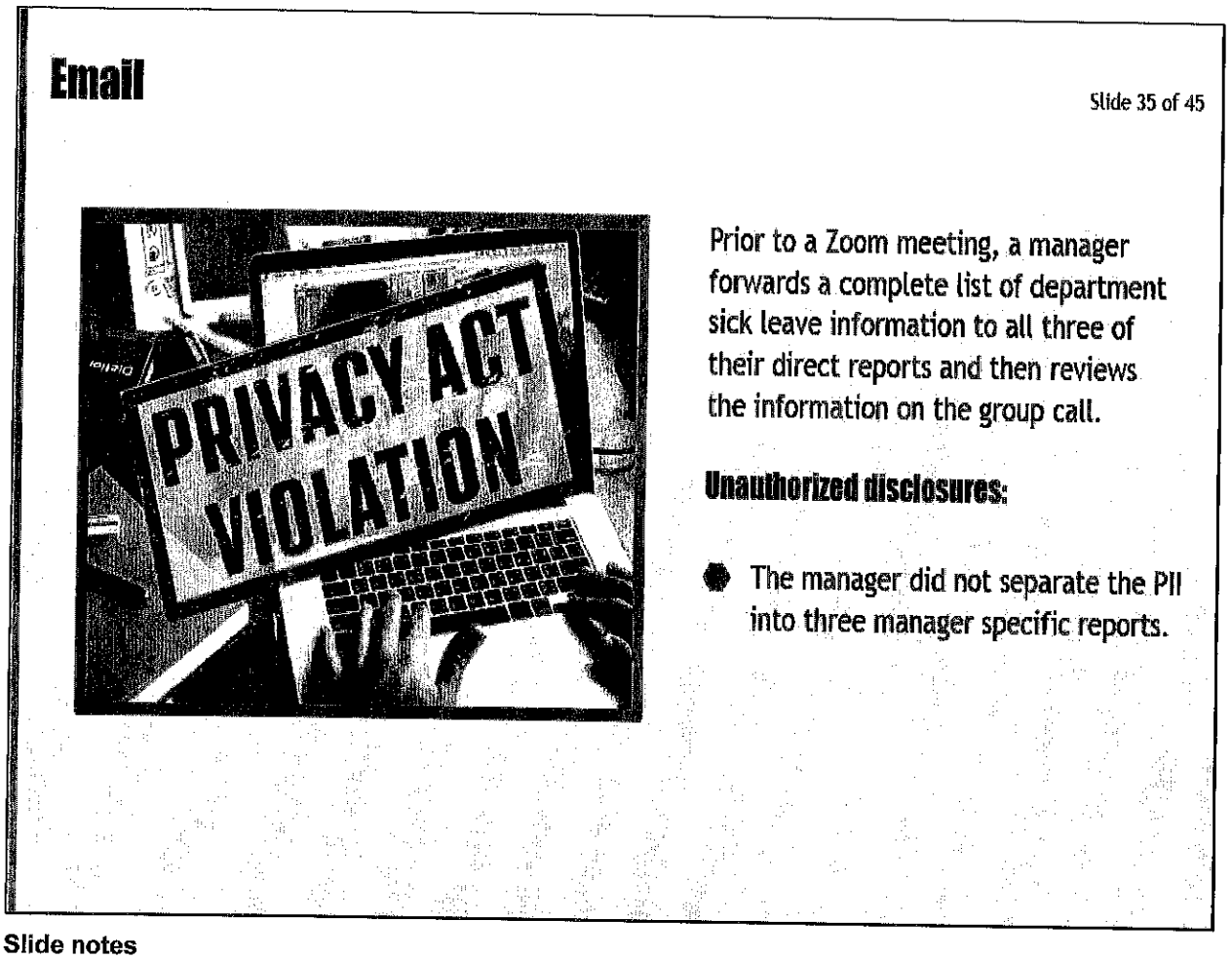
Slide notes

An unauthorized disclosure is an improper transfer, sharing, or exposure of information pertaining to PII of an individual.

This can happen via email, paper documents, phone calls, social media, or conversations.

Let's review more scenarios involving unauthorized disclosures.

Slide 35 - Email

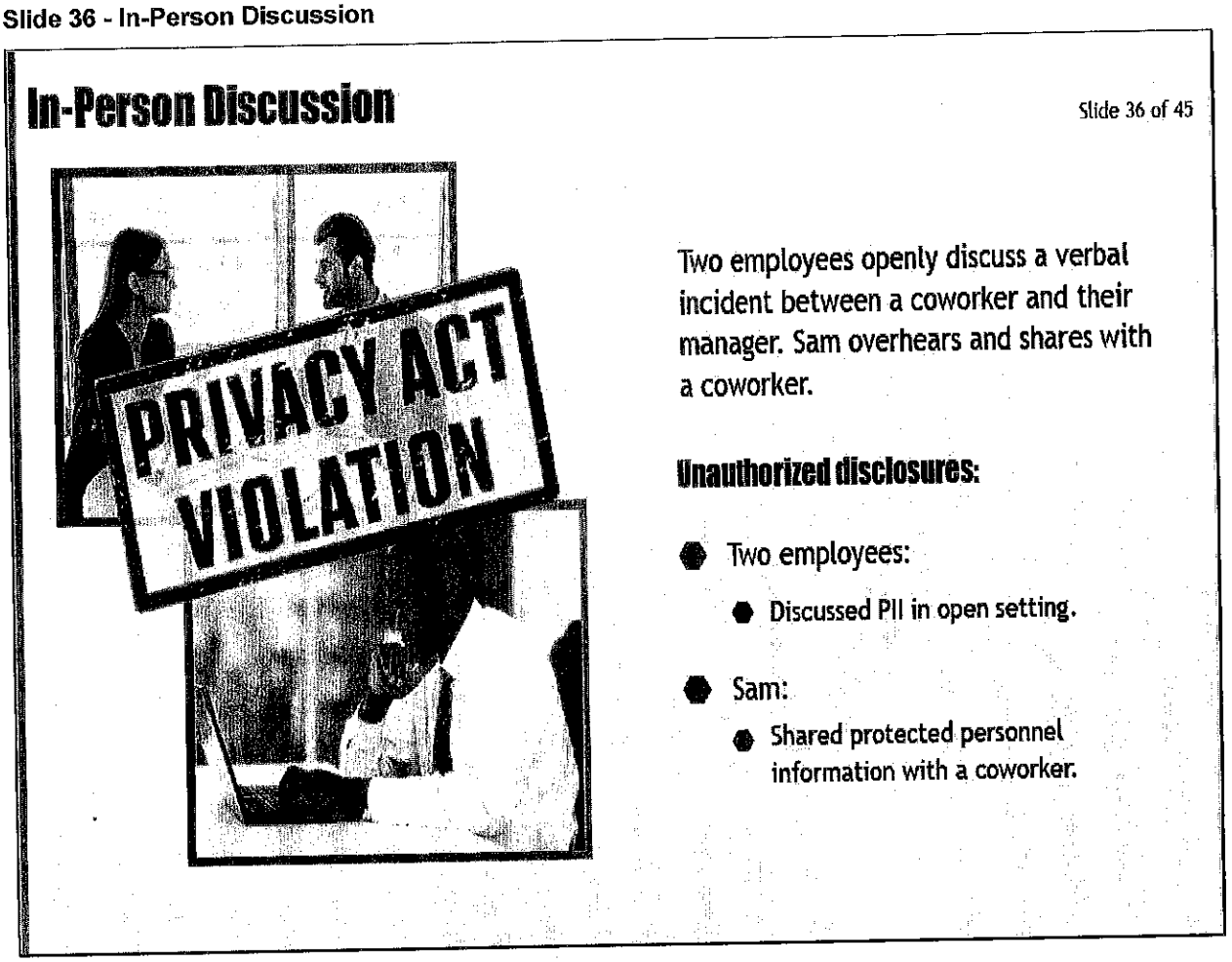


Slide notes

Prior to a Zoom meeting, a manager receives an email containing PII for all employees in their department and forwards the complete list to their three direct reports.

This means the manager made three unauthorized disclosures by not separating the personal information into three manager specific reports.

Slide 36 - In-Person Discussion



Slide notes

Two employees, sitting in an open meeting space, are discussing disciplinary actions of an employee named Tru.

Sam, working at a desk nearby, overhears the conversation and is able to identify the employee by name and department.

Sam then shares what he heard with another employee.

Since the contents of personnel files are protected under an SOR, two unauthorized disclosures were made.

The two employees made an unauthorized disclosure when they discussed PII in an open setting,

and Sam made an unauthorized disclosure to his friend.

Slide 37 - Social Media

Social Media

Slide 37 of 45

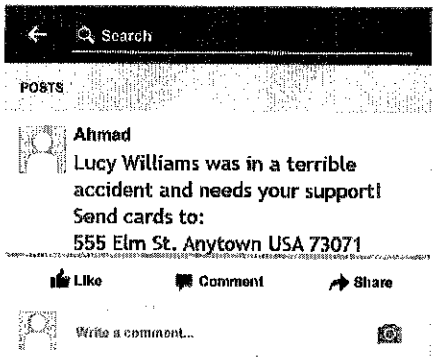
Ahmad learns a customer has been injured, so he obtains the new address from the Change of Address system.

Unauthorized disclosure:

- Address protected in USPS SOR
- Publicized full name and address

Social Media

Slide 37 of 45



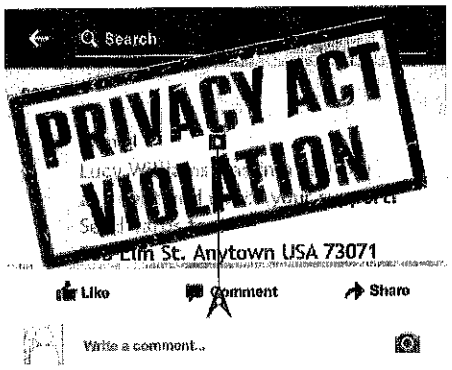
Ahmad learns a customer has been injured, so he obtains the new address from the Change of Address system.

Unauthorized disclosure:

- Address protected in USPS SOR
- Publicized full name and address

Social Media

Slide 37 of 45



Ahmad learns a customer has been injured, so he obtains the new address from the Change of Address system.

Unauthorized disclosure:

- Address protected in USPS SOR
- Publicized full name and address

Slide notes

Ahmad, a letter carrier, learns that a customer on his previous route has been injured in an auto accident.

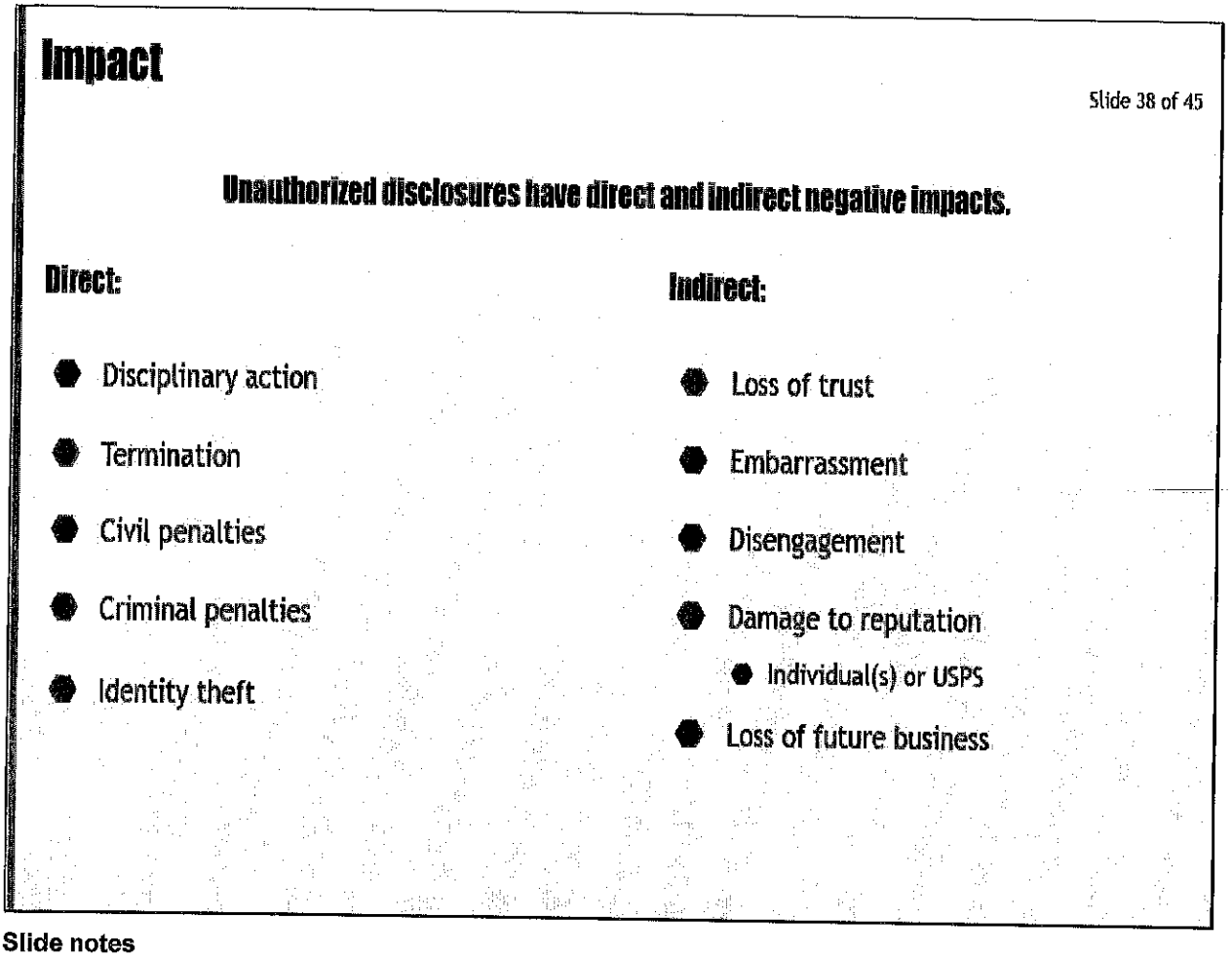
He decides it would be a good idea to have people send them cards and letters of support,

but remembers they recently moved, so he obtains the new address from the Change of Address system,

which is covered under an SOR, and publicizes the customer's full name and address on social media.

Ahmad has violated the Privacy Act by making an unauthorized disclosure of PII.

Slide 38 - Impact



Slide notes

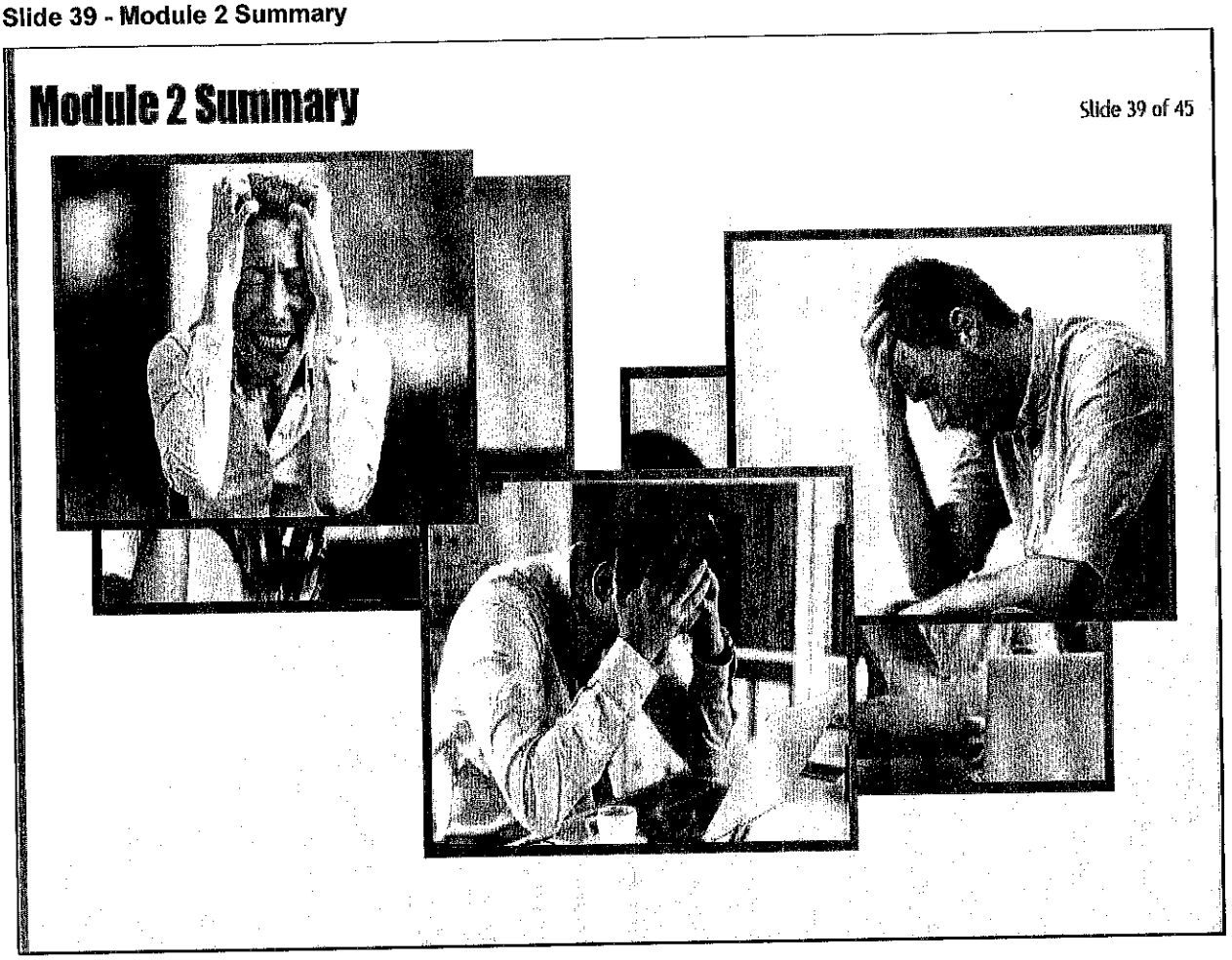
Unauthorized disclosures have direct and indirect negative impacts.

Direct consequences include, but are not limited to, disciplinary action, termination, civil penalties, criminal penalties, and even identity theft.

Less direct effects include a loss of trust, embarrassment, disengagement, damage to the reputation of individuals or USPS,

and possibly a loss of future business if the incident damages the USPS brand.

Slide 39 - Module 2 Summary

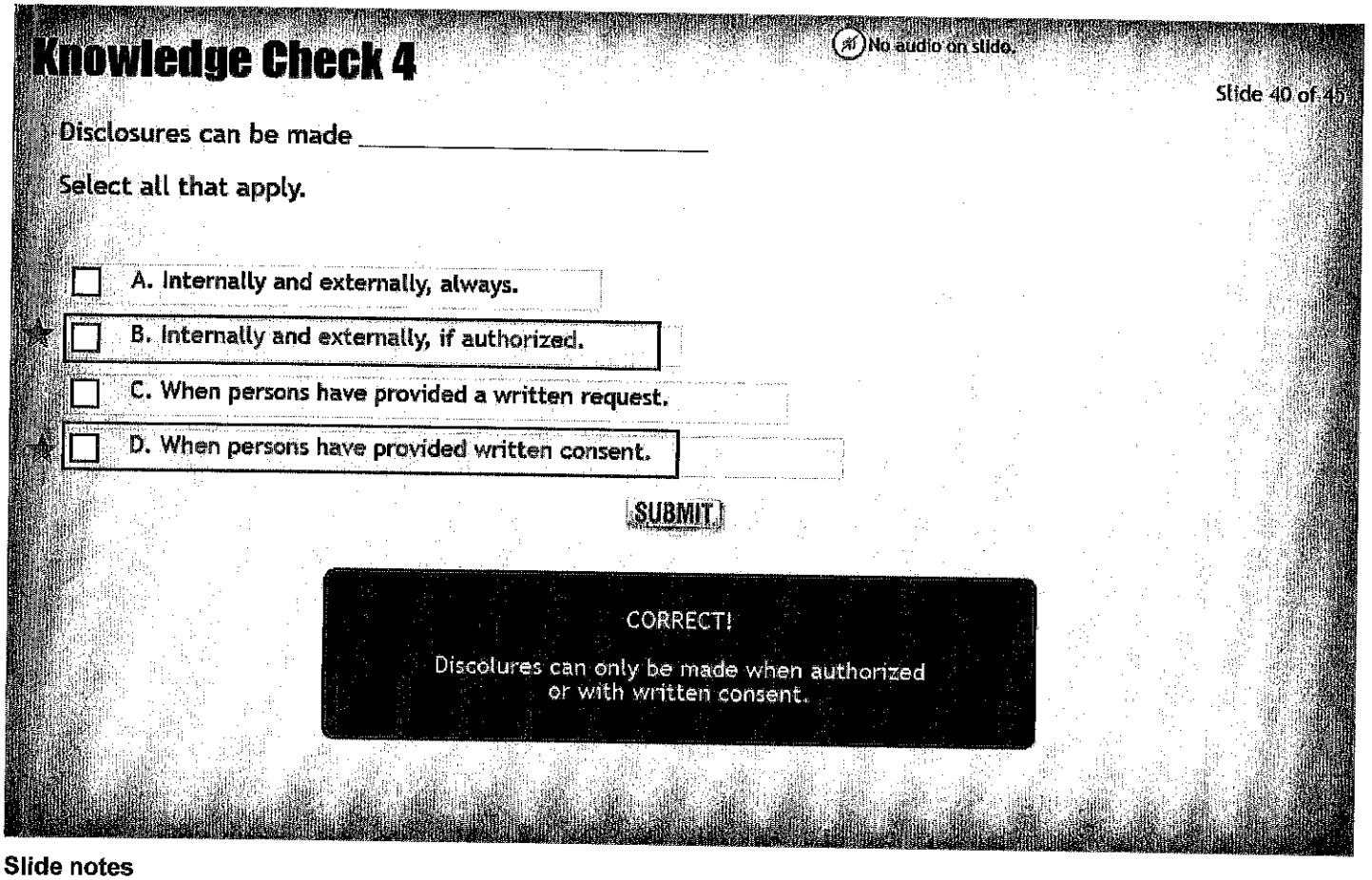


Slide notes

To review, personal information USPS collects must only be disclosed to persons who have a validated need to know or to those whom have submitted a written request for their own information.

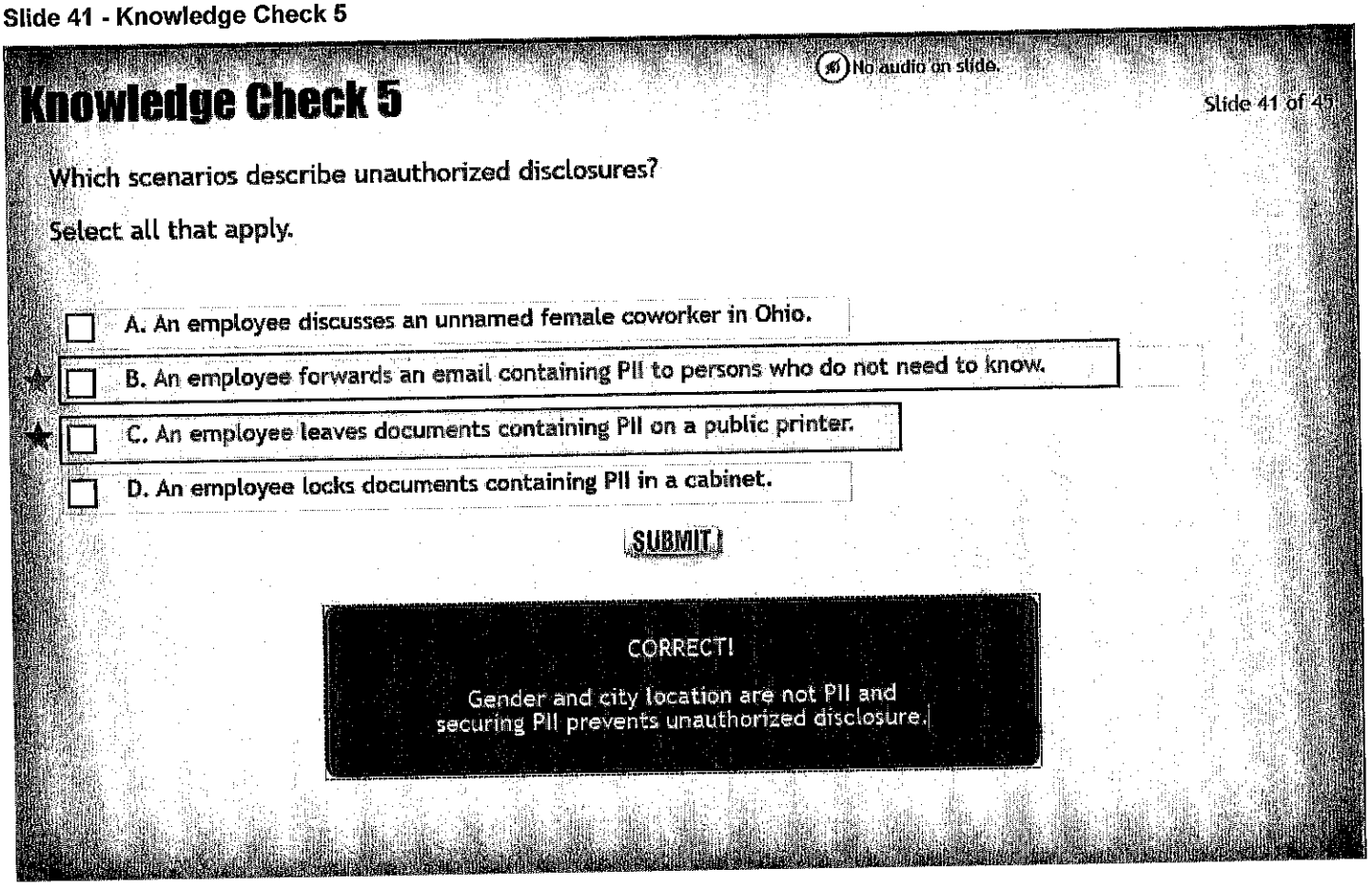
It is important to consider the very real impact of unauthorized disclosures, which could result in direct and indirect costs that negatively impact the individual and/or USPS.

Slide 40 - Knowledge Check 4



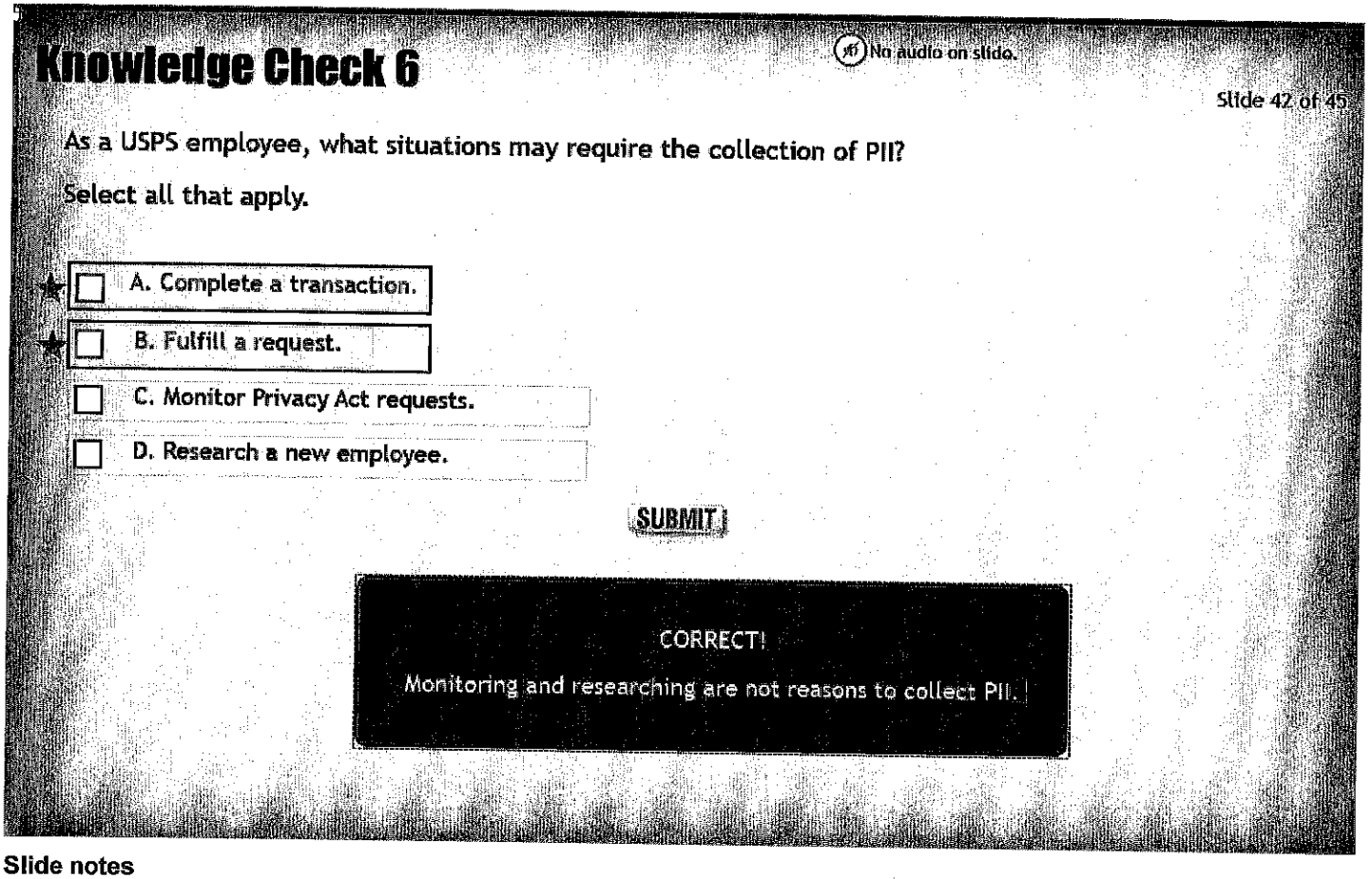
Slide notes

Slide 41 - Knowledge Check 5



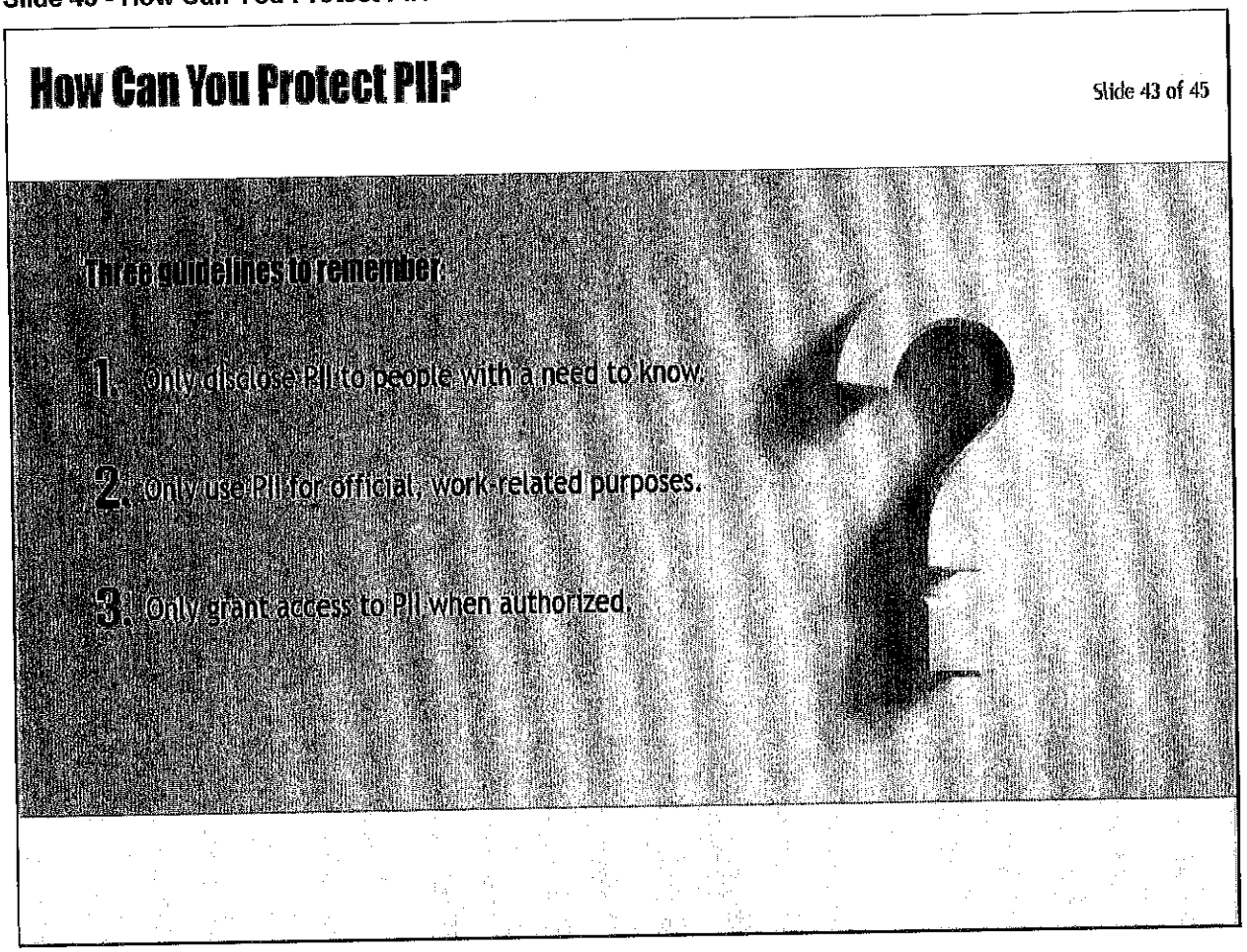
Slide notes

Slide 42 - Knowledge Check 6



Slide notes

Slide 43 - How Can You Protect PII?



Slide notes

So, how can you prevent the unauthorized access, collection, disclosure, or misuse of personal information? It's easy!

Just remember these three guidelines.

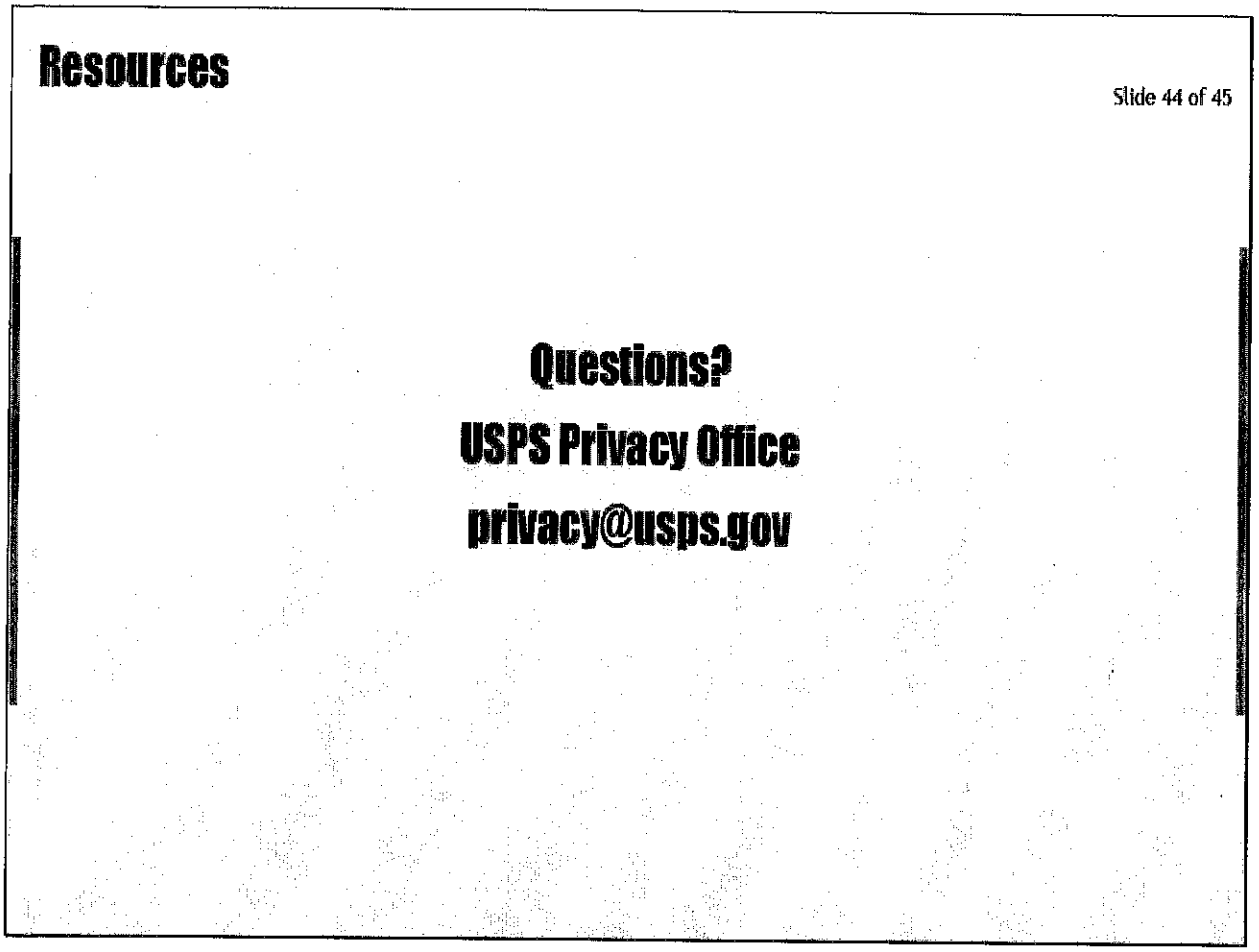
First, only disclose personal information to those who have a need to know and require the information

to perform their official duties.

Second, only use the information for official, work-related purposes.

Third, and most importantly, only grant access to PII when you're specifically authorized to do so.

Slide 44 - Resources



Slide notes

Whenever you have questions regarding a Privacy Act Statement or the USPS privacy policy,

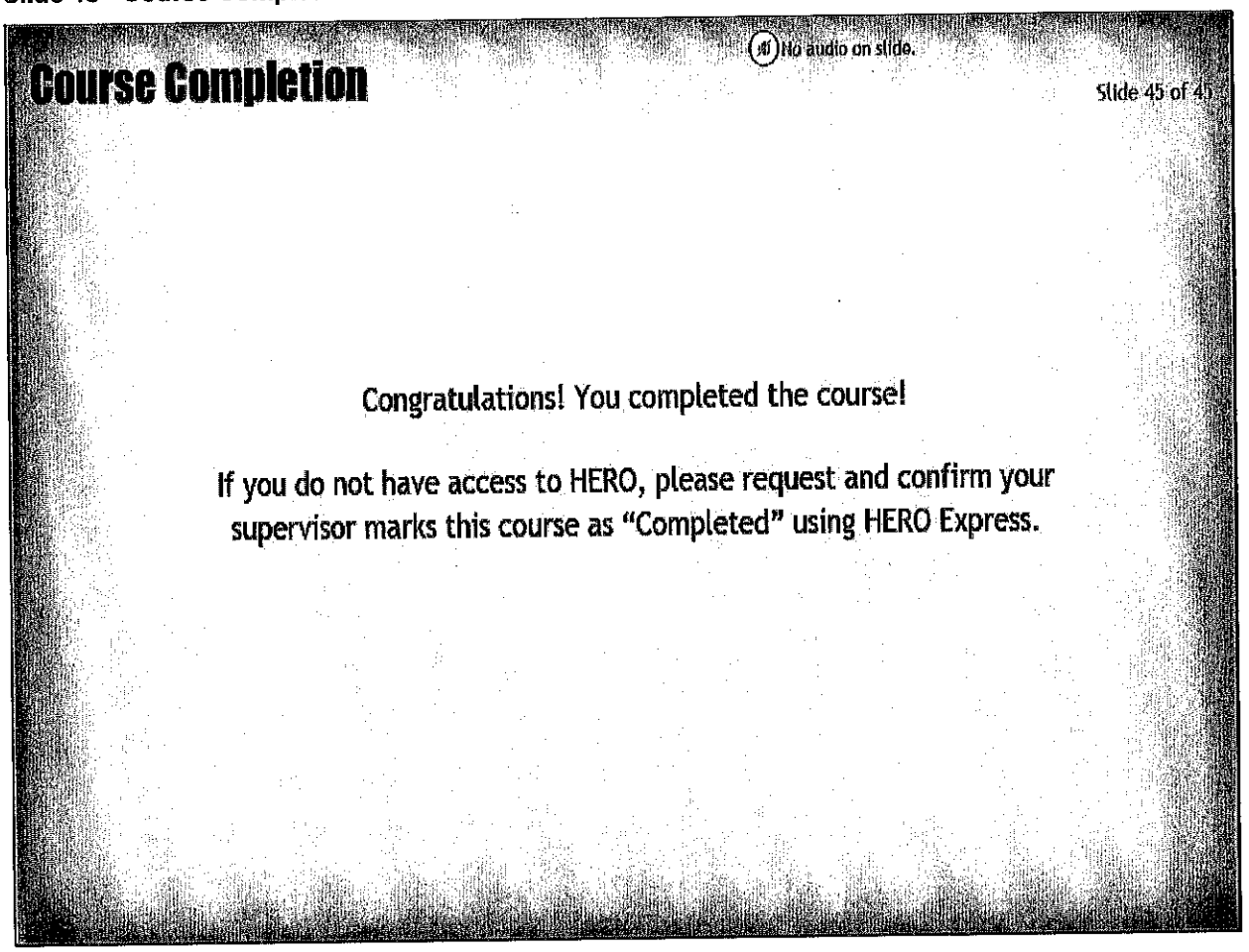
you are encouraged to contact the Privacy Office directly.

You can also find comprehensive policy details, definitions, and Privacy Act requirements

in Handbook AS-353, *Guide to Privacy, the Freedom of Information Act, and Records Management.*

Several excerpts from AS-353 were used in this course for your reference.

Slide 45 - Course Completion



Slide notes