

## Student Guide

# Assured File Transfer – Short Course

---

### Introduction

**Screen Text/Images:** At the start of the screen, are two laptops facing each other with folders appearing as if they are coming out of the screens of the laptops. On the screen appears the text, “Assured File Transfer.” Above the computers, is the screen title that reads, “Introduction.”

**Narration:** Assured File Transfer or AFT is the process of moving a file or files from a higher classification system to a lower classification system. For example, assured file transfer may be used when transferring unclassified information from a secret system to an unclassified system.

**Screen Text/Images:** On the screen, there are two computers. Under the left computer, it reads “Secret Level” and under the right computer, it reads “Unclassified Level.” On the screen of the left computer it reads, “Transferring...” On the screen of the right computer, it reads, “Receiving...” Also on the screen on the right computer, a progress bar is animating increasing red until the bar is filled. Between the two computers are two folders with an animation of documents moving from the left folder to the right folder. When the bar is completely red, the text on the left computer screen changes to “Transfer Complete,” the text and bar on the right screen disappears, and the arrows between the computers disappear.

**Narration:** If not done properly, this downloading process can easily lead to a compromise of information because of the hidden saving and storage capabilities of the software and hardware used.

**Screen Text/Images:** Image of a hand holding a magnifying glass over the screen of a computer.

**Narration:** If not done properly, this downloading process can easily lead to a compromise of information because of the hidden saving and storage capabilities of the software and hardware used.

**Screen Text/Images:** A computer and a laptop on the screen. Under the computer it reads, “Secret Level” and under the laptop it reads, “Unclassified Level.” On the monitor of the computer, an image of a file folder in the upper left corner. On the laptop monitor, an image of a file folder in the upper left corner and on the center of the monitor, it reads, “Transfer Complete.” On the top of the screen, it reads, “Assured file transferring ensures that information remains secure when released below the accredited level of the information system.”

**Narration:** However, assured file transfer uses authorized procedures to convert information into formats that can be inspected and reviewed to ensure that unauthorized information is not released at an unauthorized level.

### What is an Assured File Transfer?

**Screen Text/Images:** On the screen, there are two computers. Under the left computer, it reads “Higher Classification” and under the right computer, it reads “Lower Classification.” On the screen of the right computer, is a progress bar. Between the two computers are two folders. Between the two folders, is a green arrow pointing to the right. Above the two screens is the screen title that reads, “What is an Assured File Transfer?” Below the screen title are three bullets:

- Procedure that permits information to be released below the classification level of the information.
- If not done properly, this file transferring process can easily lead to a security compromise.
- Assured File Transfer is the set of authorized procedures that convert information into formats that can be inspected.

**Narration:** An Assured File Transfer is the procedure or series of procedures that permit identified data to be transferred from a higher classification system to a lower classification system. If not done properly, this file transferring process can easily lead to a security compromise because of hidden saving and storage capabilities of the software and hardware used. Assured File Transfer is the set of authorized procedures that convert information into formats that can be inspected in an in-depth review to ensure unauthorized information is not released at an unauthorized level.

### Who is Responsible for Assured File Transfers?

**Screen Text/Images:** At the top of the screen is the screen title that reads, “Who is Responsible for Assured File Transfers?” Under the title is the sentence, “An Assured File Transfer is performed by a Data Transfer Agent (DTA) with the assistance of a subject matter expert (SME).” Following this are a series of bullets and sub-bullets:

- The DTA is performing a security-relevant function in providing endpoint security during a transfer. DTAs must receive specialized training in AFT procedures.
  - Data review and sanitization tools
  - SCG
  - Permissible file formats
  - Authorized media formats and markings
  - Administrative record keeping
- Subject Matter Experts (SMEs)
  - Files are reviewed
  - Files are sanitized

On the right side of the screen is the text that reads, “Data Transfer Agent.” Under this text are four images; a man sitting at a laptop, a graduation cap, a woman signing a document, and a logbook with a pencil on top. Below these images is the text that reads, “Subject Matter Expert.” Under this text is an image of a woman sitting at a laptop.

**Narration:** Who is Responsible for Assured File Transfers? An Assured File Transfer can only be performed by a Data Transfer Agent (DTA) with the assistance of a subject matter expert (SME). The DTA must be trained, have written authorization, and maintain administrative records (logs) of all file transfers. The DTA is performing a security-relevant function in providing endpoint security during a transfer. DTAs must be identified in writing. AFT training for DTAs will include but is not limited to the following: Data review and sanitization tools (automated and manual). Security Classification Guide. Permissible AFT file formats. Authorized media formats and marking requirements. Procedures for AFT administrative record keeping (logs) of the transferred files. The subject matter experts are individuals knowledgeable of the program and the classification of information associated with it, and are responsible for ensuring the file are reviewed and sanitized of all program-related data.

### What are the Requirements for AFT?

**Screen Text/Images:** A series of 10 images with text under them appear on the screen one at a time.

They are:

- A man signing a piece of paper. Under it, it reads, “The file types/formats and transfer procedures must be authorized by DSS.”
- A USB flash drive in its original packaging. Under it, it reads, “Factory fresh target media.”
- An image that reads, “Scanning Files” with a progress bar under it. Under the image it reads, “All new media must be scanned for viruses.”
- A magnifying glass over a laptop screen. Under it, it reads, “A comprehensive review must be performed.”
- A box that reads, “Top Secret>Response Scenarios>Insurgent Attack.docx.” On the top of the box is a red circle, which has a red line through it. Under it, it reads, “Classified path/file links and/or classified path/file names are not used.”
- An image of words on a computer screen with puzzle pieces under it. Under it, it reads, “Files on the target media does not cause an increased classification level due to “Aggregation.” Aggregation is a link that when selected, a pop-up appears that reads, “Information, when paired with other pieces of information at the same classification level, result in a higher overall classification.”
- A person sitting in front of a computer screen. On the computer screen is an image of a file folder and a computer monitor. Under the images, it reads “TRANSFER.” Under it, it reads, “Files are transferred using an authorized utility/command.”
- An image of Windows File Explorer. Under it, it reads, “Target media is verified to contain only intended source files.”
- A woman intensely staring at a laptop screen. Under it, it reads, “Files are verified to contain the correct sensitivity of information.”

- A USB flash drive with the word, SECRET, printed on it. Under it, it reads, “Appropriate security classification labels are used.”
- A woman making an entry into a logbook. Under it, it reads, “Administrative records are kept.”

**Narration:** The file types/formats and transfer procedures must be authorized by DSS and documented in the System Security Plan. Target media must be factory fresh. All new media must be scanned for viruses with the latest definitions prior to starting the AFT. A comprehensive review must be performed to ascertain the sensitivity and classification level of the data. Classified path/file embedded links and/or classified path/file names are not used for source or target files. The compilation of all files on the target media does not cause an increased classification level due to “Aggregation.” Files are transferred using a known, authorized utility or command. Target media is verified to contain only intended source files. Files are verified on target media to contain the correct sensitivity of information and/or level of unclassified or lower classified information. The target media displays the appropriate security classification label. An administrative record of the transfer is created and maintained.

### Types of Data Transfers

**Screen Text/Images:** At the top of the screen the title reads, “Types of Data Transfers.” Under it, it reads, “There are two types of data transfers:” Below the text, there are two sets of two computers. To the left of the two upper computers, a button appears with the text, “Low-to-High” on it. To the left of the two lower computers, a button appears with the text, “High-to-Low” on it.

On the screen of the left computer (upper set of computers) it reads, “Receiving...” On the screen of the right computer, it reads, “Transferring...” Also on the screen on the right computer, is a progress bar. Between the two computers are two folders. Between the two folders is a green arrow pointing to the left.

On the screen of the left computer (lower set of computers) it reads, “Transferring...” On the screen of the right computer, it reads, “Receiving...” Also on the screen on the right computer, is a progress bar. Between the two computers are two folders. Between the two folders is a green arrow pointing to the right.

**Narration:** There are two types of data transfers. Low to High. And High to Low. Select each data transfer type to learn more.

When the Low-to-High button is selected, a pop-up is displayed.

**Pop-up Screen Text/Images:** In the pop-up, it reads, “Low-to-High. Low-to-High is defined as a transfer from a lower classification system to a higher classification system, and includes data transferred between two like security domains. Select the icon to open the Assured File Transfer Job Aid. Then there is a pdf icon link. Under the text is the same image of the upper set of computers as was on the screen.

When the High-to-Low button is selected, a pop-up is displayed.

**Pop-up Screen Text/Images:** In the pop-up, it reads, “High-to-Low. High-to-Low is defined as a transfer from a higher classification system to a lower classification system. It includes a transfer between systems of the same classification with a differing set of programs. Select the icon to open the Assured File Transfer Job Aid. Then there is a pdf icon link. Above the text is the same image of the lower set of computers as was on the screen.

### **Authorized File Types and Formats**

**Screen Text/Images:** At the top of the screen the title reads, “Authorized File Types and Formats.” Under it, it reads, “Select each tab to see a description of the file type/formats” Below the text, are five tabs. The first tab reads, “ASCII.” The second tab reads, “HTML.” The third tab reads, “JPEG.” The fourth tab reads, “BITMAP.” The fifth tab reads, “GIF.”

**Narration:** DSS authorized file type/formats include: ASCII, HTML, JPEG, BITMAP, GIF. Now let’s take a look at each of the file types. Select each tab to reveal a description of the file type/formats and an example of the converted file.

When the ASCII tab is selected:

**Screen Text/Images:** Text on the left reads, “ASCII-formatted information is essentially raw text. Many applications have the ability to export data in ASCII or text format. Program source code, batch files, macros and scripts are straight text and stored as ASCII files that may be read with any standard text editor. Common file extensions include, but are not limited to, .txt, .dat, .c, .for, .fil, .asc, and .bat.” To the right is an image of an ASCII document with a banner that reads, “Jog Aid.txt.”

**Narration:** ASCII-formatted information is essentially raw text. Many applications have the ability to export data in ASCII or text format. Program source code, batch files, macros and scripts are straight text and stored as ASCII files that may be read with any standard text editor. Common file extensions include, but are not limited to, .txt, .dat, .c, .for, .fil, .asc, and .bat.

When the HTML tab is selected:

**Screen Text/Images:** Text on the left reads, “The document format used on the World Wide Web. Web pages are built with HTML tags (code) embedded in the text. HTML defines the page layout, fonts, and graphic elements, as well as the hypertext links to other documents on the Web. Common file extensions include .html and .htm.” To the right is an image of an HTML page with a banner that reads, “CDSE.html.”

**Narration:** The document format used on the World Wide Web. Web pages are built with HTML tags (code) embedded in the text. HTML defines the page layout, fonts, and graphic elements, as well as the hypertext links to other documents on the Web. Common file extensions include .html and .htm.

When the JPEG tab is selected:

**Screen Text/Images:** Text on the left reads, “JPEG (pronounced jay-peg): An ISO/ITU (International Organization of Standardization/International Telecommunication Union) standard for compressing still images that is very popular due to its high compressibility. The file extension for JPEG files is .jpg.” To the right is an image of an HTML page with a banner that reads, “computer.jpg”

**Narration:** JPEG is an ISO/ITU standard for compressing still images that is very popular due to its high compressibility. The file extension for JPEG files are .jpg and jpeg.

When the BITMAP tab is selected:

**Screen Text/Images:** Text on the left reads, “Bitmap (BMP): A Windows® and OS/2 (Operating System 2) bitmapped graphics file format. It is the Windows native bitmap format. Every Windows application has access to the BMP software routines in Windows that support it. Common file extension includes .bmp.” To the right is an image of a hard drive with a banner that reads, “Hard\_drive.bmp.”

**Narration:** Bitmap is a Windows and OS/2 bitmapped graphics file format. It is the Windows native bitmap format. Every Windows application has access to the BMP software routines in Windows that support it. Common file extension includes .bmp.

When the GIF tab is selected:

**Screen Text/Images:** Text on the left reads, “A popular bitmap graphics file format developed by CompuServe. Its common file extension includes .gif.” to the right is a hand holding a smartphone with a banner that reads, “Smartphone.gif.”

**Narration:** A popular bitmap graphics file format created by CompuServe. Its common file extension includes .gif.

### Authorized Procedures – Rules 1 through 5

**Screen Text/Images:** At the top of the screen, the title reads, “Authorized Procedures – Rules 1 through 5” Under it, it reads, “Select each rule to view a description of that rule (1-5).” Below the text, are five active tabs that reads, “Rule 1”, “Rule 2”, “Rule 3”, “Rule 4”, and “Rule 5.” Below these are grayed out tabs (inactive) for rules 6 through 13. To the right are two laptops facing each other with folders appearing as if they are coming out of the screens of the laptops.

**Narration:** There are specific rules that you will need to follow when performing an assured file transfer. It is important to follow these rules to avoid compromise due to hidden saving and storage capabilities of various software and hardware. Let’s examine these rules now. Select each rule to examine a description of that rule.

When the Rule 1 tab is selected:

**Screen Text/Images:** Text on the tab reads, “Rule 1: The target media must be factory

fresh.” Underneath is an image of USB flash drive in its original packaging.

**Narration:** Rule 1: The target media must be factory fresh.

When the Rule 2 tab is selected:

**Screen Text/Images:** Text on the tab reads, “Rule 2: The procedure must be performed by an authorized Data Transfer Agent.” Underneath is an image of a man sitting in front of a laptop.

**Narration: Rule 2:** The procedure must be performed by an authorized Data Transfer Agent.

When the Rule 3 tab is selected:

**Screen Text/Images:** Text on the tab reads, “Rule 3: If multiple files are being transferred, create a designated directory for the transfer using the DOS Make Directory command or using the new folder command under Windows File Explorer.” Underneath is an image of a computer desktop with a newly created folder called Transfer Files 5-2-18.

**Narration: Rule 3:** If multiple files are being transferred, create a designated directory for the transfer using the DOS Make Directory command or the equivalent command for your operating system or using the new folder command under Windows File Explorer.

When the Rule 4 tab is selected:

**Screen Text/Images:** Text on the tab reads, “Rule 4: If multiple files are being transferred, transfer all files into the newly created directory. This helps to ensure only the desired files are transferred.” Underneath are images of three file folders; one called Transfer Files 5-21-18, one called Forms, and one called images.

**Narration: Rule 4:** If multiple files are being transferred, transfer all files into the newly created directory. This helps to ensure only the desired files are transferred.

When the Rule 5 tab is selected:

**Screen Text/Images:** Text on the tab reads, “Rule 5: As a general rule, files should be converted to one of the acceptable formats first (DSS Authorized File Type/Formats) and then reviewed. Drawings and presentation type files (e.g., PowerPoint, Publisher, and Visio) are an exception because they can contain sensitive information hidden behind other objects such as graphics.

These types of files within their native application may have layers of information (e.g., text on top of graphics, or multiple graphic layers). Once exported into one of the authorized graphic formats (e.g., .bmp, .jpg, .gif), the layers will be merged together and will not be editable to remove any higher classified information.

To review these files:

1. Use the native application used to generate the file.

2. Ensure that every page, chart, slide, drawing, etc., of the file is examined.
3. Within each page, chart, slide, drawing etc., ensure that all layers are reviewed by ungrouping and moving objects around so everything is visible.
4. Some applications also have information in the headers and footers, notes page, etc.

**Narration: Rule 5:** As a general rule, files should be converted to one of the acceptable formats first and then reviewed. Drawings and presentation type files such as PowerPoint, Publisher, and Visio are an exception.

### Application Exercise

**Screen Text/Images:** At the top of the screen, the title reads, “Application Exercise” Below the text, is an image of a computer desktop screen with icons on the left. One of the icons is labelled strategy.pptx. There is a text box on the screen that reads, “Reviewing PowerPoint Files” followed by the sentence, “In this exercise you will review a PowerPoint file and remove any classified information and markings.”

Under that it reads:

“When reviewing PowerPoint files:

1. Review headers and footers.
2. Review the master design for the file (Master Slide).
3. Ensure there is no higher classified information hidden behind other objects.
4. Save the file in one of the authorized file formats.

Beneath the text box, a green arrow point to the left with text that reads, “Launch presentation to start the exercise” animates onto the screen. At the bottom of the screen is another text box that reads, “Select each hotspot as it appears to proceed through the exercise.” Next to the text is a purple rectangle.

**Narration:** In this exercise, you will review PowerPoint file and remove any classified information and markings.

Application Exercise:

Selecting the strategy.pptx icon brings up a simulated PowerPoint presentation. On the screen is a text box that reads, “1. Review headers and footers.” The hotspot rectangle is around the menu choice Insert. On the bottom of the screen is a magnifying glass with the word SECRET inside to indicate that is what is in the footer.

Selecting the Insert hotspot brings up the Insert menu with the hotspot rectangle around the Header & Footer menu choice.

Selecting the Header & Footer hotspot opens the Header and Footer dialog box with the hotspot rectangle around the Footer option. Selecting the Footer hotspot removes the word SECRET from the Footer field and the hotspot rectangle moves around the Apply to All option. Selecting the Apply to All hotspot removes the dialog box and the word SECRET from the footer. This also brings up the second slide in the presentation.

On the screen is a text box that reads, “2. Review the master design for the file (Master Slide).” The hotspot rectangle is around the View menu choice.

Selecting the View hotspot brings up the View menu with the hotspot rectangle around the Slide Master menu choice. Selecting the Slide Master hotspot opens the Slide Master screen with the hotspot rectangle around the text, “This presentation contains SECRET information.” Selecting the hotspot rectangle brings up a Delete button. Selecting the Delete button removes the sentence, “This presentation contains SECRET information.” The hotspot rectangle button is around the menu choice Close Master View. Selecting the Close Master View hotspot closes the Master Slide screen and displays the third slide of the presentation.

On the screen is a text box that reads, “3. Ensure there is no higher classified information hidden behind other objects.” The hotspot rectangle is around the image on the slide. Selecting the hotspot selects the image. Selecting the hotspot around the image again, move the image to the left and shows the text, “Secret Information” along with a Delete button. Selecting the Delete button removes the text, “Secret Information.” Selecting the hotspot around the image, moves the image back to its original place.

The fourth slide appears with a text box that reads, “4. Save the file in one of the authorized file formats.” The hotspot rectangle is around the menu option File. Selecting the File hotspot opens the Info screen with the hotspot rectangle around the Save As option. Selecting the Save As hotspot opens the Save As screen with the hotspot around the Desktop folder. Selecting the Desktop hotspot opens the Save As dialog box with the hotspot rectangle around the PowerPoint Presentation (\*.pptx) option in the Save as type field. Selecting the hotspot changes the file name from strategy.pptx to strategy.jpg and in the Save as type field in now reads “JPEG File Interchange Format (\*.jpg).” The hotspot rectangle is around the Save button. Selecting the Save hotspot opens the Save dialog box with the hotspot rectangle around the All Slides button. Selecting the All Slides hotspots open a dialog box that reads, “Each slide in your presentation has been save as a separate file in the folder C:\Users\rstuffel\Desktop\strategy.jpg, with the hotspot rectangle around the OK button. Selecting the OK hotspot closes PowerPoint and returns to the desktop with a text box that reads, “Reviewing PowerPoint Files. Congratulations! You have completed this exercise.”

### **Authorized Procedures – Rule 6**

**Screen Text/Images:** At the top of the screen, the title reads, “Authorized Procedures – Rule 6” Below the title it reads, “If any files are not in one of the following five formats; ASCII/Text, HTM/HTML, JPEG, BMP, or GIF, convert it to one of these formats. If you are not familiar with how to export a particular file, check your software manual.” Rule 6 is selected and all the other rules are grayed out. Below the sentence are six tabs. Written on the tabs are:

DSS\_Budet.xlsx  
Security\_Personnel\_CONFIDENTIAL.accdb  
DSS\_Security\_Briefings.html  
Code Decipher.exe  
Security\_presentation.pptx  
Operations\_Procedures.docx

**Narration:** If a file is not in one of the following five formats: ASCII/Text, HTM/HTML, JPEG, BMP, or GIF, convert it to one. Select each file type to determine how that file type is to be treated.

When the DSS\_Budet.xlsx tab is selected:

**Screen Text/Images:** A text box appears that reads, “Spreadsheet files must be exported as an ASCII Text File.” Next to the text box is a txt icon.

**Narration:** Spreadsheet files must be exported as an ASCII text file.

When the Security\_Personnel\_CONFIDENTIAL.accdb tab is selected:

**Screen Text/Images:** In the text box, it reads, “Database files must be exported as an ASCII text file.” Next to the text box is a txt icon.

**Narration:** Database files, such as this Microsoft Access, must be exported as an ASCII text file.

When the DSS\_Security\_Briefings.html tab is selected:

**Screen Text/Images:** In the text box, it reads, “The graphics files within HTM/HTML files must be saved separately as JPG files. HTML files by themselves are text information and may be treated as a standard ASCII file format.” Next to the text box is a JPG icon.

**Narration:** The graphics files within HTM/HTML files must be saved separately as JPG files.

When the Code\_Decipher.exe tab is selected:

**Screen Text/Images:** In the text box, it reads, “Executable programs may not be transferred. The source code (ASCII text) may be reviewed/transferred to a lower-level IS and then recompiled into executable code.” Next to the text box is a txt icon.

**Narration:** Executable programs may not be transferred. The source code (ASCII text) may be reviewed/transferred to a lower-level IS and then recompiled into executable code.

When the Security\_presentation.pptx tab is selected:

**Screen Text/Images:** In the text box, it reads, “PowerPoint presentations, as well as flowchart files such as Microsoft Visio, must be exported as graphic files.” Next to the text box is a JPG icon.

**Narration:** PowerPoint presentations, as well as flowchart files such as Microsoft Visio, must be exported as graphic files, (jpeg, gif files, or bitmap files).

When the Operations\_Procedures.docx tab is selected:

**Screen Text/Images:** In the text box, it reads, “Word documents must be exported as ASCII files.” Next to the text box is a txt icon.

**Narration:** Word documents must be exported as ASCII files.

### **Authorized Procedures – Rule 7**

**Screen Text/Images:** At the top of the screen, the title reads, “Authorized Procedures – Rule 7” Below the title, it reads, “Rule 7: Review the files using a compatible application. Review all the files and not just random samples.” Under this sentence, the following bullets are displayed one at a time.

- BMP and JPG files may be reviewed with a graphics file viewer such as Microsoft Photo Editor. **Note:** Since GIF files may contain a 3D/animation/multipage image, you must use a program that will show all the information stored in GIF files. Internet Explorer can be used to display GIF files. Microsoft Photo Editor will not display all the frames (images) and therefore is not adequate to view GIF files.
- For ASCII text, the preferred application for reviewing is NotePad. However, these applications have file size limitations. If the file cannot be opened in NotePad, use Microsoft Word.
- After completing your review, remove all encoded formatting created by previous editing with Microsoft Word. On the file menu, select Save As (Selected Approved Format) and then select Save.
- Review remaining ASCII files not viewable with NotePad with Microsoft Word.
- For all file formats, verify the source and target file names are not classified.

**Narration:** Rule 7: Review the files using a compatible application. Review all the files and not just random samples.

BMP and JPG files may be reviewed with a graphics file viewer such as Microsoft Photo Editor. **Note:** Since GIF files may contain a 3D/animation/multipage image, you must use a program that will show all the information stored in GIF files. Internet Explorer can be used to display GIF files. Microsoft Photo Editor will not display all the frames (images) and therefore is not adequate to view GIF files.

For ASCII text, the preferred application for reviewing is NotePad. However, these applications have file size limitations. If the file cannot be opened in NotePad, use Microsoft Word.

After completing your review, remove all encoded formatting created by previous editing with Microsoft Word. On the file menu, select Save As (Selected Approved Format) and then select Save.

Review remaining ASCII files not viewable with NotePad with Microsoft Word.

For all file formats, verify the source and target file names are not classified.

### **Authorized Procedures – Rule 8 through 13**

**Screen Text/Images:** At the top of the screen, the title reads, “Authorized Procedures – Rules 8 through 13” Under it, it reads, “Select each rule to view a description of that rule (8-13).” Below the text, are five active tabs that read; “Rule 8”, “Rule 9”, “Rule 10”, “Rule 11”, “Rule 12”, and “Rule 13.” Above these are grayed out tabs (inactive) for rules 1 through 7. To the right are two laptops facing each other with folders appearing as if they are coming out of the screens of the laptops.

**Narration:** Select each rule to view a description of that rule.

When the Rule 8 tab is selected:

**Screen Text/Images:** Text on the tab reads, “Rule 8: Use the standard save or transfer command or utility (e.g., drag and drop, copy, etc.) to transfer the files to the target media.” Underneath is an image of folder being drag to a folder on another drive.

**Narration:** Rule 8: Use the standard save or transfer command or utility to transfer the files to the target media.

When the Rule 9 tab is selected:

**Screen Text/Images:** Text on the tab reads, “Rule 9: Write-protect the media (physical or software) as soon as the transfers are complete.” Several locks sitting on a keyboard.

**Narration:** Rule 9: Write-protect the media as soon as the transfers are complete.

When the Rule 10 tab is selected:

**Screen Text/Images:** Text on the tab reads, “Rule 10: Verify (dir/s [drive]: or Windows File Explorer) that only intended files were transferred.” Underneath is an image of Windows File Explorer with two pdf files to the right.

**Narration:** Rule 10: Verify that only intended files were transferred.

When the Rule 11 tab is selected:

**Screen Text/Images:** Text on the tab reads, “Rule 11: Compare the files that were transferred to the originals [fc pathname/filename) drive: (path/filename)].” Underneath are images of two instances of Windows File Explorer. The top image has two pdf files with the words Flash Drive. The bottom image has the same two pdf files with the word Original.

**Narration:** Rule 11: Compare the files that were transferred.

When the Rule 12 tab is selected:

**Screen Text/Images:** Text on the tab reads, “Rule 12: Apply the appropriate security classification label to the target media.” Underneath is an image of a USB flash drive with the word SECRET written on it.

**Narration:** Rule 12: Apply the appropriate security classification label to the target media.

When the Rule 13 tab is selected:

**Screen Text/Images:** Text on the tab reads, “Rule 13: Create an administrative record of the transfer and maintain it with your audit records. The record must specify the data being released, the personnel involved, and the date.” Underneath is an image of a woman writing in a logbook.

**Narration:** Rule 13: Create an administrative record of the transfer and maintain it with your audit records. The record must specify the data being released, the personnel involved, and the date.

### Summary

**Screen Text/Images:** At the top of the screen, the title reads, “Summary” Under it, it reads, “Assured File Transfers ensure that information remains secure when released below the classification level of the information system.”

Below the sentence are two computers. Under the left computer, it reads “Secret Level” and under the right computer, it reads “Unclassified Level.” On the screen of the left computer it reads, “Transferring...” On the screen of the right computer, it reads, “Receiving...” Also on the screen on the right computer, a progress bar is animating increasing red until the bar is filled. Between the two computers are two folders with an animation of documents moving from the left folder to the right folder. When the bar is completely red, the text on the right computer screen changes to “Transfer Complete,” the text on the left screen disappears and bar on the right screen disappears, and the folders between the computers disappear.

**Narration:** This short examined the procedures for assured file transfer. You must be vigilant in following these procedures to ensure that classified information is protected and safeguarded.

### Conclusion

**Screen Text/Images:** At the top of the screen, the title reads, “Conclusion” Under it is a text box that reads, “Congratulations! You have completed the Assured File Transfer Short.”

Below the sentence are two laptops facing each other with folders coming out of both screens.