Student Guide
Assured File Transfer – Short Course

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.

Screen Text/Images: The title “Assured File Transfer” appears onscreen between two laptops facing each other with folders appearing as if they are coming out of the screens of the laptops.

Next, two computers appear onscreen. The desktop computer on the left is labeled "Secret Level" and the other laptop computer is labeled "Unclassified Level."

Narration: For example, assured file transfer may be used when transferring unclassified information from a secret system to an unclassified system.

Screen Text/Images: Information appears on each of the computer screens. The desktop Secret Level screen states “Transferring" and the laptop Unclassified Level screen states "Receiving" and shows a progress bar with an increasing red marker until the bar is filled in red.

Between the two computers are two folders with an animation of documents moving from the left folder to the right folder.

When the progress bar is completely red, the text on the Unclassified Level computer screen changes to "Transfer Complete," the text and bar on the Unclassified Level computer 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: Next an image of a hand holding a magnifying glass over the screen of a computer appears.

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.

Screen Text/Images: The images of the Secret Level and Unclassified Level computers re-appear with “Transfer Complete” showing on the Unclassified Level computer.

Who Is Responsible for Assured File Transfers?

Screen Text/Images: An Assured File Transfer is performed by a Data Transfer Agent (DTA) with the assistance of a Subject Matter Expert (SME). An image of a man sitting at a laptop in an office appears onscreen labeled "Data Transfer Agent." Additional images appear onscreen:

- Graduation cap
- Person signing a document
- Logbook with a pencil on top

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
- Security Classification Guide
- Permissible file formats
- Authorized media formats and markings
- Administrative record keeping

An image of a woman sitting at a laptop labeled "Subject Matter Expert" appears onscreen.

Subject Matter Experts (SMEs)

- Files are reviewed
- Files are sanitized

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 that the files are reviewed and sanitized of all program-related data.

What Are the Requirements for AFT?

Screen Text/Images: Images and captions appear onscreen with a blue line slowly building and linking each image/caption as the narration describes them:

- A man signing a piece of paper with caption "The file types/formats and transfer procedures must be authorized by DCSA."
- A USB flash drive in its original packaging with caption "Factory fresh target media."

- Screenshot stating “Scanning Files” with a progress bar under it with caption “All new media must be scanned for viruses.”
- Magnifying glass over a laptop screen with caption “A comprehensive review must be performed.”
- File location “Top Secret>Response Scenarios>Insurgent Attack.docx” with a red “do not enter” symbol over it and caption “Classified path/file links and/or classified path/file names are not used.”
- Words on a computer screen with puzzle pieces under them with caption “Files on the target media do not cause an increased classification level due to ‘Aggregation.’”
- A person viewing a computer screen showing images of a file folder and a computer monitor with “TRANSFER” appearing prominently onscreen. Caption is “Files are transferred using an authorized utility/command.”
- Image of Windows File Explorer with caption “Target media contains only intended source files.”
- A woman intensely staring at a laptop screen with caption “Files are verified to contain the correct sensitivity of information.”
- A USB flash drive with the word SECRET printed on it and caption “Appropriate security classification labels are used.”
- A woman making an entry into a logbook with caption “Administrative records are kept.”

Rollover

Aggregation: Information, when paired with other pieces of information at the same classification level, result in a higher overall classification.

Narration: The file types/formats and transfer procedures must be authorized by DCSA 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: There are two types of data transfers:

Images appear of two sets of two computers; one set is next to a button labeled “Low-to-High” and the other set is next to a button labeled “High-to-Low.”

The “Low to High” set of computers has a desktop computer next to a laptop computer. The desktop screen shows the message “Receiving.” The laptop screen shows the message

"Transferring" along with a progress bar. Between the two computers are two folders. Between the two folders is a green arrow pointing from the laptop to the desktop.

Similarly, the "High-to-Low" set of computers has a desktop computer next to a laptop computer. The desktop screen shows the message "Transferring." The laptop screen shows the message "Receiving" along with a progress bar. Between the two computers are two folders. Between the two folders is a green arrow pointing from the desktop computer to the laptop.

Select each type to learn more.

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.

Image of two computers: a desktop computer next to a laptop computer. The desktop screen shows the message "Receiving." The laptop screen shows the message "Transferring" along with a progress bar. Between the two computers are two folders. Between the two folders is a green arrow pointing from the laptop to the desktop.

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.

Image of two computers: a desktop computer next to a laptop computer. The desktop screen shows the message "Transferring." The laptop screen shows the message "Receiving" along with a progress bar. Between the two computers are two folders. Between the two folders is a green arrow pointing from the desktop computer to the laptop.

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

Authorized File Types and Formats

Screen Text/Images: Five file tabs appear onscreen labeled as follows:

- ASCII
- HTML
- JPEG
- BITMAP
- GIF

Select each tab to see a description of the file type/formats.

Narration: DCSA 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: Image of an ASCII document appears onscreen labeled "Job Aid.txt" 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.

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: Image of an HTML page appears onscreen labeled "CDSE.html" HTML is 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.

Narration: HTML is the document format used on the World Wide Web. Web pages are built with HTML tags (or 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: Images of a laptop, tablet, and cellphone screens appear onscreen labeled "computer.jpg" JPEG is 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 extensions for JPEG files are .jpg and .jpeg.

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

When the BITMAP tab is selected:

Screen Text/Images: Image of a hard drive appears onscreen labeled "Hard_drive.bmp" Bitmap (BMP): A Windows® and OS/2 (Operating System 2) bit mapped 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. The common file extension is .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 is .bmp.

When the GIF tab is selected:

Screen Text/Images: Image of a person holding a smartphone appears onscreen labeled "Smartphone.gif" GIF is a popular graphic file format developed by CompuServe. Its common file extension is .gif.

Narration: GIF is a popular graphic file format created by CompuServe. Its common file extension is .gif.

Authorized Procedures – Rules 1 through 5

Screen Text/Images: Image appears onscreen of two laptops facing each other with folders appearing as if they are coming out of the screens of the laptops. Select each rule to view a description of that rule (1-5)

Narration: There are specific rules that you will need to follow when performing an assured file transfer. It is important to follow these rules and 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 the rule.

When the Rule 1 tab is selected:

Screen Text/Images: The target media must be factory fresh. 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: The procedure must be performed by an authorized Data Transfer Agent. 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: 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. 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: If multiple files are being transferred, transfer all files into the newly created directory. This helps to ensure only the desired files are transferred. 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: As a general rule, files should be converted to one of the acceptable formats first (DCSA 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.

Select Next to continue.

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: Image of a computer desktop screen with icons on the left. One of the icons is labeled "strategy.pptx".

Reviewing PowerPoint Files

In this exercise you will review a PowerPoint file and remove any classified information and markings.

When reviewing PowerPoint files be sure to:

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.

Launch presentation to start the exercise. 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 a PowerPoint file and remove any classified information and markings.

Screen Text/Images: 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 moves 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 it 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 opens a dialog box that reads, "Each slide in your presentation has been saved 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.

Reviewing PowerPoint Files.

Congratulations! You have completed this exercise."

Authorized Procedures – Rule 6

Screen Text/Images: 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.

Six selectable tabs:

- DCSA_Budget.xlsx
- Security_Personnel_CONFIDENTIAL.accdb
- DCSA_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 DCSA_Budet.xlsx tab is selected:

Screen Text/Images: TXT icon. Spreadsheet files must be exported as an ASCII Text File.

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

When the Security_Personnel_CONFIDENTIAL.accdb tab is selected:

Screen Text/Images: TXT icon. Database files must be exported as an ASCII text file.

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

When the DCSA_Security_Briefings.html tab is selected:

Screen Text/Images: JPG icon. 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.

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: TXT icon. 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.

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

When the Security_presentation.pptx tab is selected:

Screen Text/Images: JPG icon. PowerPoint presentations, as well as flowchart files such as Microsoft Visio, must be exported as graphic files.

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: TXT icon. Word documents must be exported as ASCII files.

Narration: Word documents must be exported as ASCII files.

Authorized Procedures – Rule 7

Screen Text/Images: Review the files using a compatible application. Review all the files and not just random samples. The following bullets are displayed as the narration plays:

- 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: Select each rule to view a description of that rule. (8-13)

Image of 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: Use the standard save or transfer command or utility (e.g., drag and drop, copy, etc.) to transfer the files to the target media. Image of folder being dragged 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: Write-protect the media (physical or software) as soon as the transfers are complete. Image of 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: Verify (dir/s [drive]: or Windows File Explorer) that only intended files were transferred. Image of Windows File Explorer displaying icons of two pdf files.

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

When the Rule 11 tab is selected:

Screen Text/Images: Compare the files that were transferred to the originals [fc pathname/filename) drive: (path/filename)].

Images of two instances in Windows File Explorer. The top image has icons of two pdf files labeled “Flash Drive.” The bottom image has the same icons of two pdf files, and these are labeled “Originals.”

Narration: Rule 11: Compare the files that were transferred to the originals.

When the Rule 12 tab is selected:

Screen Text/Images: Apply the appropriate security classification label to the target media. 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: 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. 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: Assured File Transfers ensure that information remains secure when released below the classification level of the information system.

Two computers appear onscreen. The desktop computer on the left is labeled “Secret Level” and the other laptop computer is labeled “Unclassified Level.”

Information appears on each of the computer screens. The desktop Secret Level screen states “Transferring” and the laptop Unclassified Level screen states “Receiving” and shows a progress bar with increasing red until the bar is filled.

Between the two computers are two folders with an animation of documents moving from the Secret Level computer to the Unclassified Level computer.

When the progress bar is completely red, the text on the Unclassified computer screen changes to “Transfer Complete,” the text and bar on the Secret Level computer disappears, and the arrows between the computers disappear.

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

Conclusion

Screen Text/Images: Congratulations! You have completed the Assured File Transfer Course. Image of two laptops facing each other with folders coming out of both screens.

Narration: Congratulations! You have completed the Assured File Transfer Course.