TRUSTED DOWNLOAD

Background

Trusted download refers to a procedure, or series of procedures, that permits information to be released below the accredited level of the Information System (IS).

Almost without exception, the majority of contractors Information Systems that are accredited to process classified information operate at Protection Level (PL) 1 or PL 2. As such, the protection requirements identified in Section 6 of NISPOM Chapter 8 do not support more than one classification and/or sensitivity level of information. Simply stated, the IS cannot recognize or distinguish information based on content. All information residing or processed on a PL 1, 2 or 3 IS are handled/treated at the classification/sensitivity level for which the IS is accredited.

Scope

The February 2006 NISPOM Chapter 8 requirements for trusted download shall be implemented by all newly accredited or reaccredited ISs at PL1, PL2, or PL3 that require the transfer of information with different sensitivities or information with unclassified or lower classified information. The implementation of the trusted download requirements will provide contractors with specific guidelines on how to perform this task while maintaining an acceptable level of risk during the creation of lower-than-system-level output.

In general, DSS trusted download requirements include:

- A comprehensive review by a “Knowledgeable User” (see definitions)
- The applicable DSS standard file type/formats and file transfer procedures documented in the IS System Security Plan (SSP)

• Where authorized on the DD-254 or as a contract line item, alternate detailed procedures included in the IS SSP which constitutes an acknowledgement and acceptance of additional risk from the government customer/data owner.

NISPOM Requirements

The following Chapter 8 requirements apply to Trusted Downloading:

8-310a. Human-Readable Output Review. An appropriate sensitivity and classification review shall be performed on human-readable output before the output is released outside the security boundary to determine whether it is accurately marked with the appropriate classification and applicable associated security markings.

8-310b. Media Review. Electronic output, such as files, to be released outside the security boundary shall be verified by a comprehensive review (in human-readable form) of all data on the media including embedded text (e.g., headers and footer) before being released. Information on media that is not in human-readable form (e.g., embedded graphs, sound, video, etc.) will be examined for content using the appropriate software application. CSA-approved random or representative sampling techniques may be used to verify the proper marking of large volumes of output.

Definitions

1. Aggregation. The generation of a higher level overall classification of information when combining two or more lower level classified files (e.g. the combination of two unclassified files on a media producing Confidential or SECRET media) based on Security Classification Guide(s), restriction(s).

2. Acknowledgement of Risk. Alternative Trusted Downloading Procedures that do not follow the DSS guidelines may be used only when the Government Customer/data owner has formally (in writing) acknowledged and accepted the risk inherent in the alternate file type/format and procedures.

3. Comprehensive Review. A methodical review to ensure that all higher level information has been removed prior to the data being released outside the IS's security boundary. Comprehensive Reviews fall into two categories: Hardcopy and media. For hardcopy output a review shall be performed by a "Knowledgeable User" to determine the correct classification and portion marking of the information. For large products in human-readable form, the comprehensive review must be done on no less than 20% of the output product. For media output, the media shall be created by a "Knowledgeable User" following the DSS "File Transfer Procedure" as defined in the IS's SSP.

4. Knowledgeable User. An IS user (general or privileged) who is considered a data matter expert with extensive knowledge of all appropriate

security classification guide(s), and who can perform the “Comprehensive Review”. The User shall be trained by the Information System Security Manager (ISSM) or Information System Security Officer (ISSO) in understanding the vulnerabilities associated with producing lower-than-system-level output and file transfer procedures.

5. Sensitivity. Refers to formal access requirements (e.g., NATO, COMSEC, CNWDI) or caveats that specify handling or releasability restrictions (e.g., Foreign Government Information (FGI).

6. Slack Space. The data storage space that exists from the end of a file to the end of the last cluster assigned to the file. Slack space potentially can contain randomly selected bytes of classified data from computer memory.

7. Trusted download. A procedure, or series of procedures, that permits information to be released below the accredited level of the Information System (IS). Release of information outside the IS may take the form of hardcopy (or human-readable), digital/analog media, or electronic transfer.

File Type/Formatting Issues

The many different file formats represent a security challenge to the contractor, DSS, and in many cases the Government Contracting Activity (GCA) or data owner. For the most part every application, even those belonging to a professional software suite (e.g., Microsoft Office, Mat Lab, Claris) formats, stores, displays, and/or codes information differently. Some use proprietary coding techniques, some hide file related information (in binary and/or ASCII format) within the file, and some do things from a DSS security viewpoint that even the vendor cannot explain. However, to perform a reliable “trusted download”, existing file format vulnerabilities must be considered.

While no security procedures can mitigate 100% of the risk involved, the DSS approved Trusted Download procedures mitigate an acceptable amount of risk and have been tested to ensure the reliability of the procedures.

The only “SAFE” method of removing unclassified information from a classified system is to print and perform a comprehensive human review by a “Knowledgeable User”. Once the printed output is reviewed, it is a simple process to scan the document into an unclassified or lower classified information system. This will eliminate the vulnerabilities associated with electronic media.

No matter which file type/formats are used, the SSP must identify the file format(s) and specific procedures for reviewing and transferring those formats.

Legacy Operating Systems Slack Space Issues

In addition to File Type/Format issues, there is also an issue with how certain Operating Systems handle slack space that must be considered

when copying information to media or during electronic transfers. Systems that are known to produce slack space with non-predictable results are:

- MAC (note: does not include MAC X O/S)
- Windows 95
- Windows 95, release A
- Some early versions of Windows 98

When copying to media or performing electronic transfers from these operating systems a DSS-authorized copy product/procedure must be used.

DSS Authorized File Type/Formats

This Policy supports both hardcopy and media/electronic transfer file type/formats.

Hardcopy:
All human-readable output sent to hardcopy devices, such as printers, copiers and faxes, independent of the original files format, fall into this category. This includes, but is not limited to, ASCII, HEX and Octal files, word processing, graphics, database and scientific files. As long as the file can be reviewed meeting the "Comprehensive Review" criteria it is eligible for release at a level (i.e., classified or unclassified) lower than the accredited IS level.

Media/Electronic Files:
The following file formats are authorized by DSS to be released from the IS at or below the IS's accreditation level without an acknowledgement of risk from the government customer, but only after a comprehensive review:

Format Type	Explanation	Common File Extension(s)
ASCII	ASCII formatted information is essentially raw text just like the words you're reading now. 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. ASCII files may be read with any standard text editor.	**.txt .dat .c .for .fil .asc .bat** Note: This is not an all-inclusive list. If a file cannot be read with a standard text editor, try changing the extension to **.txt**. If the file still cannot be read with a text editor, it is most likely not an ASCII file.
Hypertext Markup Language	The document format used on the World Wide Web. Web pages are built with HTML tags (codes) 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.	**.html .htm**
JPEG	Joint Photographic Experts Group (pronounced jay-peg) An ISO/ITU standard for compressing still images that is very popular due to its high compression capability.	**.jpg**

BMP	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.	**.bmp**
Graphics Interchange Format	A popular bitmapped graphics file format developed by CompuServe.	**.gif**

DSS File Transfer Procedures

For every file type or format, there are an endless number of transfer procedures that have been developed by industry and government. Some of the more common ones are identified at the end of this document. What's important to remember about these or any alternate procedure is that the contractor must get the GCA or data owner to acknowledge the increased risk to classified information created by using one of the non-DSS authorized file types/formats and/or procedures.

No matter what file format or procedure is used, there are requirements that are common to all general media and to electronic transfers:

1. The file types/formats and transfer procedures must be certified by DSS and documented in the SSP.

2. Target media must be factory fresh.

3. A comprehensive review must be performed so as to ascertain the sensitivity and classification level of the data.

4. Classified path/file embedded links and/or classified path/file name(s) are not used for source or target file(s).

5. The compilation of all files on the target media does not cause an increased classification level due to "Aggregation".

6. File(s) are transferred using a known, authorized utility or command.

7. The target media is verified to contain only intended source file(s).

8. File(s) are verified on target media to contain the correct sensitivity of information and/or level of unclassified or lower classified information.

9. The appropriate security classification label is applied to the target media.

10. An administrative record of the transfer is created and maintained.

DSS Authorized Procedure (Windows-Based)

1. The target media must be new.

2. The procedure must be performed by a “Knowledgeable User”.

3. If multiple files are being transferred, create a designated directory for the transfer using the DOS make directory command (md [drive:] path) or the new folder command under Windows Explorer. [Rationale: This will establish an empty directory which helps ensure that only intended files are transferred.]

4. If multiple files are being transferred, transfer all files into the newly created directory.

5. As a general rule, files should be converted to one of the acceptable formats first (DSS Authorized File Type/Formats), then reviewed. Drawings and presentation type files (e.g. PowerPoint, Publisher, and Visio) are an exception. These types of files within their native application may have layers of information, for example text on top of graphics, or multiple graphics layered together. Once exported into one of the authorized graphic formats (i.e. .bmp, .jpg, .gif) the layers will be merged together and will not be editable to remove any higher classified information. To review these files use the native application used to generate the file. Ensure that every page, chart, slide, drawing etc. of the file is examined. Within each page, chart, slide, drawing, etc. ensure that all layers are reviewed by ungrouping and moving objects around so everything is visible. Some applications may also have information in headers and footers, notes pages, etc. Below is a detailed procedure for reviewing one of the more commonly used presentation/graphic applications, PowerPoint:

a. Review Headers and Footers. To do this: Click on **Header and Footer** under the **View** menu. Click on and review both the **Slide** and the **Notes and Handouts** tab.

b. Review the Masters for the file. To do this: Click on **Master** under the **View** menu. Then select and review each of the Masters (Slide, Title, Handout, & Notes).

c. For each slide, click on **Edit**, then **Select All**. Once all objects are selected, click on **Draw** (bottom left of screen), then **Ungroup**, until the Ungroup option is no longer available (grayed out). Hit the tab key to outline each object (delineated by a box around a graphic or text), in the slide. If an object is outlined but not visible, move it, bring it forward or change its color until it is visible, or delete it. Repeat this process for each object in the slide. Use this process to find and delete all higher classified information.

d. After the review is complete, save the information in one of the authorized formats. To do this: Click on **File Save As** under the **File** menu. Select one of the DSS authorized formats from the drop-down menu of **Save As Type**.

6. If any files are not in one of the following four formats, ASCII/Text, HTM/HTML, JPEG, BMP, GIF, convert it to one of these formats.

a. Spreadsheet and database files must be exported as an ASCII text file(s).

b. 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.

c. Executable programs may not be transferred. The source code (ASCII text) may be reviewed/transferred to a lower level IS then re-compiled into executable code.

7. Review the file(s) using a compatible application. Review the entire file(s) not just random samples.

a. BMP and JPG files may be reviewed with a graphics file viewer such as MS Photo Editor. (Note: because GIF files may contain a 3D/animation/multi-page image, you must use a program that will show all the information stored in GIF files. Internet Explorer or

Netscape can be used. MS Photo Editor will not display all the frames (images) and therefore is not adequate to view GIF files).

b. For ASCII text, the preferred application for reviewing is NotePad. However, these applications have file size limitations. If the file may not be opened with NotePad, then use MS Word (step d below).

c. After completion of the review, remove all encoded formatting created by previous editing with MS Word. To do this: On the **File** menu**,** click **Save As…. (Selected Approved Format)** then click **Save**.

d. Review remaining ASCII files not viewable with NotePad with MS Word:

(1) Ensure all hidden text and codes are viewable. To do this: Click **Options** on the **Tools** menu, click the **View** tab, then select every option under the **Show** section and **All** under **the Formatting Marks** section.

2) Verify all Tracked changes (Revisions in MS Word) are viewable. To do this: Click on **Track Changes** then **Highlight Changes** under the **Tools** menu,. If Enabled, Disable the **Track changes while editing**. Enable the **Highlight changes on screen**.

(3) Review the Summary and Contents sections of the file properties. To do this: Click **Properties** on the **File** menu, then click on the **Summary** and **Contents** tabs.

(4) Review Headers and Footers. To do this: Click on **Header and Footer** under the **View** menu. Headers will be displayed at the top of each page, any footers will be displayed at the bottom of each page. Note: If a document has multiple Sections, each Section may have different Headers and Footers.

(5) Review Comments. To do this: Click on **Comments** under the **View** menu. A comments pane will be displayed at the bottom of the screen. If Comments is grayed out under the View menu, this means there are no comments within the document.

(6) Review Footnotes: To do this: Click on **Footnotes** under the **View** menu. If Footnotes is grayed out under the View menu, this means there are no footnotes within the document. If footnotes are not grayed out there are footnotes. If you are displaying the document in Normal layout or Web Layout, a footnote pane will appear at the bottom of the screen. If you are displaying the document in Print Layout, footnotes will already be visible at the bottom of each page, or at the end of the document.

(7) Review the entire contents of the file including all Sections. All embedded objects except clipart and WordArt must be deleted. When reviewing clipart and WordArt and text boxes ensure there is no information hidden behind these objects. Note: Embedded objects may be opened and saved separately prior to deletion. Each separately saved object is subject to this procedure prior to transfer.

(8) When you are finished reviewing the file, ensure all hidden deleted information from Fast Save operations is removed. To do this: On the **File** menu**,** click **Save As …(Selected Approved Format)** then click **Save**. Also, if the file is not yet in one of the acceptable file format types, select one of the DSS approved formats from the drop-down menu of **Save As Type**.

e. For all file formats, verify the source and target file(s) names are not classified.

8. Use the standard save or transfer command or utility (i.e. drag and drop, copy, etc) to transfer the file(s) to the target media.

9. Write-protect the media (physical or software) as soon as the transfer(s) are complete.

10. Verify (dir/s [drive]: or Windows Explorer) that only intended file(s) were transferred.

11. Compare the file(s) that were transferred to the original(s) [fc (pathname/filename) drive: (path/filename)].

12. Apply the appropriate security classification label to the target media.

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

DSS Authorized Procedure (Unix)

Note: These procedures should be tailored for the local environment. In particular, the Unix commands listed herein are for illustration only and must be modified to account for the Unix version, hardware configuration, and software installation specifics.

1. Target media must be new.

2. Procedure must be performed by a “Knowledgeable User”.

3. If multiple files are being transferred, create a designated source directory for the transfer using the Unix make directory command (mkdir directory_name). Rationale: This will establish an empty directory. This two-step process helps ensure that only intended files are copied.

4. If multiple files are being transferred, transfer all files into the newly created directory.

5. Verify the source and target file(s) names are not classified.

6. View the contents of all file(s) in the designated directory, not just “random samples.”

a. For text files use software that displays the entire contents of the file. (EG: Hex editor) Any unintelligible data is assumed to be classified at the accredited IS level.

b. For graphics or movie files review the file(s) using an appropriate file viewer. Ensure that the file format does not include internal annotations or other additional data (if present, this information can only be viewed with a specialized viewer, and poses a significant threat of inadvertent disclosure).

c. For non-text files the sensitivity or classification of non-text, non-graphics files cannot generally be determined without intensive technical analysis. Such files must be assumed to be classified. Files in this category include binary database files, compressed archives, and executable code.

(1) In the case of executable files, review and downgrade the source code, then transfer the source code to a lower-classified machine for re-compilation.

(2) In some cases, the source code will be classified, but the compiled code will be unclassified as specified in the classification guidance document. After compilation, the executable must be reviewed with HEX editor software to ensure that no classified information has escaped the compilation process.

(3) In the case of binary database files, export the data to ASCII text format, then review and downgrade the text file for media migration.

(4) Compressed archives should be reviewed and transferred uncompressed.

7. Use the Tar utility to create and write an archive of the source directory to the target media. The Unix command sequence will be as shown below (the exact command may vary depending on the Unix version, machine configuration, and the media used):

mt -f /dev/rst0 rew	Ensure tape is rewound (not required if using floppy)
tar cvf /dev/rst0 /directory_name	Create Tar file on tape

8. Write-protect the media as soon as the transfer(s) are complete.

9. Verify that the media contains the expected data by printing a directory of the Tar file:

mt -f /dev/rst0 rew Ensure tape is rewound (not required for floppy)

tar tvf /dev/rst0 | lpr Print directory of file (| lpr may be omitted for on-screen review)

10. The output of the above command should match the contents of the source directory. To verify that they match, compare the output of the above command with the directory printed by the following command:

ls -alR /source-directory | lpr (| lpr may be omitted for on-screen review)

11. Ensure the date, time, and file size(s) are as expected. If any unintended data was copied, the target media must be considered classified and cannot be used for a trusted down load again.

12. Apply the appropriate security classification label to the target media.

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

Trusted Download Authorization

I certify that the individual identified below has been briefed in the vulnerabilities associated with transferring unclassified or lower classified information off of an accredited Information System (i.e. trusted download). Additionally, they have demonstrated extensive knowledge of all information they will download.

Name:_____ Date: _____

Authorized File Format(s)

ISSM/ISSO Signature:_____ Date:_____