Office of Compliance

Digital Image Guidance for EPA Civil Inspections and Field Investigations

Number: OECA-GUID-2017-001-R1
06/13/2017
U.S. Environmental Protection Agency

Page Intentionally Blank

Revision History

This table shows changes to this controlled document over time. The most recent version is presented in the top row of the table. Previous versions of the document are maintained by the OECA Document Control Coordinator.

History	Effective Date
Digital Image Guidance for EPA Civil Inspections and Field Investigations, Revision 1 Revisions to reflect changes in technology (e.g. memory devices and formatting) and EPA policies (e.g. information security and records management).	06/13/2017
Digital Image Guidance for EPA Civil Inspections and Field Investigations, Original Issue	2006

CONTENTS

DISCLAIMER

This Guidance has been developed for federally-credentialed inspectors acting on behalf of the U.S. Environmental Protection Agency (EPA) and is intended solely for internal management purposes. It does not create any rights, substantive or procedural, enforceable at law. EPA may periodically revise this Guidance to make improvements and/or to reflect changes in EPA policy. EPA reserves the right to act at variance with this Guidance. Variances must be explained and documented. Varying from this Guidance does not disqualify the use of information obtained, for any purpose.

PURPOSE OF GUIDANCE

The purpose of this Guidance is to establish EPA procedures for generating, storing and preserving digital images for civil inspections and field investigations. In addition to this Guidance, each Regional office using digital cameras or similar equipment as part of inspections and investigations may develop a Standard Operating Procedure (SOP) with regionally-tailored steps governing the use of digital cameras or similar equipment (A model SOP template is provided in Appendix A of this document). EPA staff, grantees and contractors should look to general records and litigation hold requirements in the instances where this Guidance does not apply, such as when capturing digital images outside of civil inspections or investigations.

Digital images may be used to document conditions observed during civil inspections and investigations (herein referred to as "inspections"). Digital image means any photograph or video taken using a digital camera or device, including the audio portion of the video. Inspections are conducted to evaluate a regulated entity or the regulated portion of that facility for the purpose of gathering information to determine if it is in compliance with applicable environmental requirements. Inspections may also assess a regulated entity's ability to maintain compliance. Inspections do not include visits to a regulated facility or site for the purpose of providing compliance assistance.[1] An investigation is a detailed assessment of a regulated entity's compliance status over days or a longer period, which requires significantly more time to complete than a typical inspection. Investigations may include extensive file reviews. Investigations may also include responses to citizen tips and complaints and evaluations of areas where potentially illegal disposals, discharges, etc. have occurred. For purposes of this document, emergency response operations and removal activities are considered field investigations.

This Guidance is intended for use by EPA staff and for grantees and contractors who perform inspections on behalf of EPA. If an EPA employee, grantee or contractor chooses to vary from a provision of this Guidance because it is determined to be inappropriate, inadequate and/or impractical, such variance must be explained and documented. Choosing to vary from, or inadvertently failing to follow, a provision of this Guidance does not disqualify information obtained for any purpose including administrative or judicial proceedings. This document provides the core elements and basic structure for using digital images, and regions and programs may have additional guidance in their region/program-specific SOP.

[1] Even though compliance assistance visits are not considered to be inspections, this guidance may be applied to Agency activities besides civil inspections and field investigations where violations are discovered and digital images are taken for potential enforcement purposes.

Note: The word "must" designates activities that EPA employees are expected to perform for purposes of national consistency. The words "should" or "may" designate recommendations that EPA employees are strongly encouraged to follow.

If there are questions about this Guidance, the person responsible for such digital images should consult with the Office of Compliance. This Guidance supersedes the July 2006 Digital Camera Guidance for EPA Civil Inspections and Investigations (EPA 305-F-06-002).

INTRODUCTION

This Guidance applies to EPA-purchased digital cameras as well as digital cameras integrated into tablets and other electronic devices issued by EPA. Digital images must not be taken with personally owned devices.

Inspection reports often include digital images taken during the inspection to support an inspector's observations. To be effective, a digital image must be of sufficient clarity and detail to reflect the inspector's observations, and must represent what the inspector saw with the appropriate level of detail. The integrity of a digital image in court (i.e. evidence) is dependent on answering a simple question: Is this a fair and accurate representation of what was observed?

This Guidance sets forth procedures necessary to ensure the integrity of the digital images. This document addresses digital image capture, storage, printing and handling. Appendix A contains a model SOP for the use of digital images. Appendix B contains examples of Digital Image Logs and Digital Image Modification Logs. Appendix C contains National Archives and Records Administration (NARA) requirements regarding preferred and acceptable formats for digital images.

The use of digital images as evidence in court will depend on EPA's ability to show reliability, reproducibility, and security. It is generally acceptable to make minor changes, such as cropping, enlarging, or other post processing, to a working copy of the digital images, to improve the ability to identify what is being captured in the image, without distorting its evidentiary value. The minor changes also include making the image clearer or sharper by adjusting certain parameters, such as light/darkness and contrast. However, the unaltered original image must be preserved. Generally, the inspector should:

- Follow a written SOP developed by the applicable Regional or HQ office that includes the required and recommended steps set forth in this document;
- Ensure that the digital image accurately captures what the inspector observed;
- Record how, when, and where the digital image was taken;
- Preserve the original digital image (also known as the "archival copy" or "the copy of record");
- Maintain documentation for the archival digital image files;
- Log the steps used in processing the working copy of the digital image in a Digital Image Modification Log or other accompanying notes; and
- Use only working copies of digital images in inspection reports and other enforcement support documents.

Technical Information

The following information includes a discussion of some important factors to consider when using digital cameras and before going on an inspection. The minimum requirements necessary for good quality images will change as technology changes.

Resolution

Digital resolution is the amount of sharpness or detail in the digital image and is dependent on the number of pixels in the digital image. The higher the resolution, the higher the digital image quality, but the more storage space the digital image will use. Pixels are the unit used to measure resolution.

Higher pixel levels allow creation of digital images with a high level of detail that will not be lost if the digital image is enlarged. This is important where larger digital images may be necessary and/or where greater detail is important. The quality of a printed digital image is only partially dependent on the camera resolution. Printer resolution capability is also an important factor when printing digital images.

Power Supply

Digital cameras may use nickel metal hydride (NiMH rechargeable batteries), nickel cadmium (NiCd, rechargeable), lithium (non-rechargeable), or alkaline (nonrechargeable). Of these, the NiMH batteries are currently the most economical because of their low cost, rechargeability, length of charge, and long service life. (They are also environmentally preferable to the nickel cadmium batteries which are gradually being phased out). The lithium batteries are useful as cold-weather back-ups.

Optical Zoom

Another factor affecting digital image quality, particularly for close-ups or distance, is optical zoom. Optical zoom is “true zoom” or telephoto, which makes the digital image appear closer without losing detail. Cameras with a higher degree of optical zoom allow for a greater degree of flexibility in use without loss of image quality. Digital zoom is really just built in image enlargement with some resulting loss of digital image detail.

Storage Media/Memory

A digital camera uses and/or contains random access memory (RAM) to store the digital images. When RAM is used up, it should be restored in order to take more digital images. There are several types of storage media used to record digital images. Digital images can be downloaded and stored in many places, including a computer’s hard drive, CD, cloud server, network server, and flash drive.

The number of digital images, which can be taken per session depends on the resolution selected and the amount of memory available in the digital camera and/or storage media used for the digital camera. This is somewhat dependent on the file format used. Most digital cameras use a file format, which “compresses” the digital image so that more digital images can be stored on the storage media.

There are two file types used to store images on the storage media. A “lossless” or uncompressed file is one where no data is lost. Two file format types frequently used by digital

cameras to capture "lossless" images are TIFF (Tagged Image File Format) and RAW[2] (that has not been altered, processed or manipulated in any way). "Lossless" or uncompressed files tend to be quite large.

Another file type in which some data may be lost is known as a "lossy" or compressed file. Images stored this way take up much less room but may lose some data or picture quality. However, the resultant "loss" may not be significant to over-all image quality.

One common type of "lossy" file format that is currently used by most digital cameras is a standard file format known as JPEG (Joint Photographic Experts Group). At the highest JPEG resolution, even though there may be some small loss of picture quality, it would not be obvious to the human eye and may be acceptable for inspectors. (This is less true for images of things like signs or other very hard-edged objects.) When the camera saves files in the JPEG format, the amount of compression (image quality) must be decided upon.

Most cameras give you the option in the setup menu to choose the JPEG image quality. The decision is a compromise between picture quality and the number of files that can be fit on a memory card. As with other files, higher quality "lossy" files will produce a higher quality video, but will take up more space on the digital camera. Most original video files recorded on a digital camera are proprietary "lossy" files. "Lossy" files may be appropriate to use if sufficient detail is not lost. Also note that when the image is captured for the first time and compressed in a JPEG, this is where the loss occurs. Subsequent opening/viewing/copying the file does not typically result in loss of data unless additional compression or change in file format, by the user, occurs after the image has been captured.

Most digital cameras come with a built-in image file identifier (which assigns a unique number to each picture), date, and time stamps. This is an important feature which can be helpful for record-keeping purposes.

PROCEDURE

The following section provides required and recommended procedures for EPA staff, grantees and contractors to follow when using digital images to document EPA civil inspections and investigations.

Note: If a facility does not allow an inspector to capture images during an inspection, please refer to the statutory authority under which the inspection is being conducted, EPA's general practices and procedures regarding inspector access, and contact your region or program office legal point of contact for access issues.

[2] RAW is not an acronym. A raw image file contains minimally processed data from the image sensor of a digital camera. Raw files are named so because they are not yet processed and therefore are not ready to be printed or edited with a bitmap graphics editor. Normally, the image is processed by a raw converter where precise adjustments can be made before conversion to a file format such as TIFF or JPEG for storage, printing, or further manipulation. Raw image files are sometimes called "digital negatives," as they fulfill the same role as negatives in film photography: that is, the negative is not directly usable as an image, but has all of the information needed to create an image. The purpose of raw image formats is to save, with minimum loss of information, data obtained from the sensor, and the conditions surrounding the capturing of the image (the metadata).

A. Taking and Recording the Digital Image

- Required Procedures
  - Set and verify the camera's date and time settings (where applicable) with the correct date and time in the location of the facility/site.
  - After capturing the digital image, check for clarity as practicable and confirm relevant details, such as readily identifiable unique items, objects, events, actions, or activities, and any other relevant information.
  - Take another image if the digital image is not an accurate portrayal or does not capture the relevant details.
  - Document any rare circumstance in which a digital image is deleted during an inspection (e.g., the image inadvertently captures confidential business information (CBI) that is not necessary for the inspection, digital image is claimed as CBI and inspector is not authorized to receive CBI material, image inadvertently includes facility staff which conflicts with facility policy, etc.) and, if practicable, retake an image that avoids the concern.[3]

- Recommended Procedures
  - Use the lowest level of image compression to create high quality images.
  - Take at least one image with the camera body perpendicular to the object with the camera's image sensor parallel to the object.
  - Have an extra charged battery(s) and battery charger with you when using a digital camera for inspections.
  - If an inspector decides to save files as JPEGs, it is recommended that the inspector select the camera setting that delivers the highest quality (lowest compression level) and the largest image size.
  - Confirm the type of file formats your computer's graphics editing software can use prior to selecting a digital image file format.
  - Capture images from multiple angles of the scene if necessary. For example, it may be helpful to take wide, medium, and close-up shots to capture additional details of the subject being photographed.
  - Provide scale to a scene or object of interest by placing a familiar object (e.g. penny, clipboard, pen, etc.) in the photo. This helps the viewer understand the size and scale of a scene/object.
  - If practicable, the inspector should record the date/time the digital image was taken by using a time stamp if it will not obscure any evidence that is being recorded by the image. If it may obscure evidence, then this information can also be captured in the metadata.

3 It is strongly recommended that digital images not be deleted. Images captured by mistake, that are blurry, or out of focus should be maintained as a matter of record and to help preserve metadata.

- View the image on the camera to ensure the digital image accurately depicts the inspector's observations. Consider pairing the digital camera with a GPS unit to identify the location of the images, which can assist in mapping those images.

B. Requirement to Log Digital Images

It is required that the inspector keep a record in the inspection file of all the digital images taken. This record may be a list of the digital images noted as part of the field notes, a separate digital image list, or a separate Digital Image Log. Of these, the recommended record is a Digital Image Log. It is recommended that the camera's built-in file identifier be used to identify the images in the log.

The Log must include any subsequent modifications made to any digital image thereafter or a separate Modification Log must be kept that lists the subsequent modifications made to the digital image. A log of modifications is only required for those images that were modified. See below for more information on what information must be included in the Modification Log. The record must be detailed enough to allow the inspector or another experienced individual to readily explain and easily reproduce the final modified image.

Appendix B of this Guidance provides examples of Digital Image Logs and Digital Image Modifications Logs.

As an alternative to maintaining a Digital Image Log or Digital Image Modification Log, inspectors may instead choose to use the camera's function settings to capture the required metadata described below in subparagraph numbers 2 and 3 for each digital image, or use the computer folders which house those digital images, after an inspection.

1. The record of digital images must identify all the digital images taken during an inspection, including the archival copies[4] and working copies[5]. This is separate from the field notes.

2. The record of digital images must include:

- Identity of the photographer(s)/videographer(s);
- Date;
- Time;
- Location, [including information identifying the location such as facility name, address, section of the facility (e.g., 90 day storage area in back room), EPA Identification number(s));
- Brief, but relevant details of the digital images, such as readily identifiable unique items, objects, events, actions, CBI, or activities worthy of special note;
- Identifying number of the digital image; and

[4] An Archival copy is an unchanged, unedited copy of the original digital images that will be used as the permanent record. It is the functional equivalent to the "negatives" in film photography.

[5] A Working copy is a "back-up" copy of the original digital images which may be used to make minor enhancements or edits such as cropping and improving contrast

- Other relevant metadata when available, and if practicable, such as shutter speed, f-number (sometimes called focal ratio, f-ratio, f-stop, or relative aperture), ISO setting, exposure, global positioning system (GPS) coordinates, etc.

3. The record of digital image modifications or accompanying notes must include:

- Identity of the person making the modifications;
- The date modifications were made;
- Types of modifications (includes, but is not limited to cropping, reducing, enlarging, and improving contrast);
- Brief description of modifications (e.g. image was cropped to remove personnel in the picture); and
- Identifying number of the digital image.

C. Requirement to Preserve Digital Images

- Create an Archival Copy of Original Digital Images: Inspectors must create an Archival (master) Copy of all Original Image files[6] taken during the inspection as soon as practical after the digital image is captured.
    - It is required that one locks the Secure Digital (SD) or other media card used in the camera or device to prevent alterations, including those potentially made by the operating system or burning software used to make the archival copy.[7]
    - The Archival Copy must be written onto an unalterable storage media device, also known as a Write-Only Read-Many (WORM) device, such as a CD-R, DVD-R, DVD+R, or a secure electronic file stored on a secure network server, hard drive, etc., provided that proper documentation procedures are followed.
    - If a CD-R is used for Archival Copies, it must only be formatted for write-only and not be formatted as a rewritable CD or flash drive.
    - If the file is saved on a network server or hard drive, etc., it must be protected and access should be limited to the extent practical to prevent others from altering the image of the archival copy.[8] Examples of restricted access include password protection and "read only" restrictions.
    - Inspectors also may, but are not required to assign hash values[9] to the Archival Copy to authenticate that it is the original copy and prevent potential arguments of digital image alteration. Many hash functions and associated manuals on how to use the hash function are available online (See references section).

---

[6] Original Image is a file that is temporarily stored on a camera or other device.

[7] In most instances, moving digital images directly from an SD to a storage device will preserve the metadata, so the image is unaltered. If files are moved from an SD to a hard drive, then to another electronic folder, then to another storage device, metadata is more likely to be lost, potentially creating issues of authenticity.

8 It is strongly recommended that archival copies be saved to a network drive that is backed-up regularly to avoid the loss of images.

[9] A hash value is a unique identifier assigned to a file.

    - Proper documentation procedures must be in place to ensure the integrity of the Archival Copy. Make a note in your inspection file as to the location of the Archival Copy. When the Archival Copy is physically moved to a new location, make a note of that information in the inspection file.
- Creating a Working Copy for changes: After the Archival Copy has been made and protected from modification, a working copy of the digital image(s) is created to make potential modifications, to use in an inspection report, etc. If any enhancements (such as cropping or sharpening) are needed on the digital image, a Working Copy must be made from the Archival Copy. (NEVER EDIT THE ORIGINAL DIGITAL IMAGES OR ARCHIVAL COPY, INCLUDING CHANGING THE FILE NAME.)
    - The Working Copy must have a different file name to distinguish it from the Archival Copy (refer to the individual region's SOP for any naming conventions to be used when renaming Working Copies).
    - Document the alterations made to the Working Copy in the record of digital images (i.e., Digital Modifications Log) so that all enhancements can be reconstructed, if necessary. The history function of many image programs may be useful for reconstructing the image as well.
- The inspection report should clearly reflect all the file names of the images used in the report. If a naming convention is used for Working Copies, the reader will know whether the image is from an Archival Copy and is unaltered or from a Working Copy and has been altered from the Archival Copy.

D. Transferring and Printing of Digital Images

- To transfer digital images from the digital camera's memory card to the computer, a USB cord connecting the digital camera to the computer or card reader can be used.
- Make sure to lock your SD or other media card to prevent the computer from altering the date stamp on the file when it is transferred to the computer or other storage device.
- Note: The disadvantage of this method is that if the transfer is interrupted some digital images could be lost.
- Digital images can be printed at the same time they are downloaded, or printed as needed. For in-house viewing or most general purposes, viewing the digital images on a computer may be acceptable.
- To print digital images, the inspector should consider printing on archival acid free paper from a good quality color ink-jet printer using archival inks or a laser printer, particularly if the digital images will be stored for a long period of time. For high quality digital images, premium glossy photo paper will give a great degree of color accuracy, even under magnification. For general purposes plain paper, photo quality ink-jet paper, premium photo paper, etc. can be selected depending on the level of quality desired.

E. Release of Digital Images

- Facility asks to view digital images. If a facility asks to view digital images at the time of the inspection, the inspector may show the images only on government equipment.

Digital images taken during an inspection are EPA records and property of the United States Government, they are not the property of an inspected facility. In accordance with the EPA's Information Security National Rules of Behavior, only EPA-approved equipment must be used to store digital images, and EPA-owned portable media devices and resources, such as USB flash drives, must not be connected to a non-EPA media device. Similarly, non-EPA owned media devices and resources must not be connected to EPA-owned equipment. It is acceptable for facility staff to accompany an inspector and to take their own digital images of the same areas that an inspector is taking, so the facility may retain its own record of what is recorded by EPA.

- Facility asks for copies of digital images. If a facility asks for copies of digital images taken during the inspection while the inspector is still onsite, the inspector is required to advise the facility that the inspector is prohibited by EPA's Information Security National Rules of Behavior from connecting any EPA-owned portable media device or resource to any non-EPA media device. Inspectors may not use a non-authorized wireless network to download or email photos to facility representatives. A non-authorized wireless network is one that uses wireless solutions and configurations that are not configured in accordance with the EPA's Chief Information Officer's technical standards and specifically authorized by the Senior Information Official.
- The inspector may advise the facility that copies of photos may be requested through the Freedom of Information Act (FOIA) and such requests will be treated in accordance with EPA FOIA regulations at 40 CFR Part 2. Inspectors may also consult their first-line supervisor, Office of Regional Counsel or the Office of General Counsel for guidance prior to releasing digital images if they have further questions. The inspector must first create a master archival copy of all images taken as soon as practical. Once a master copy is created and a request received, management will review the images, taking into consideration whether release of the images could reasonably be expected to interfere with a possible enforcement proceeding, or disclose techniques and procedures for law enforcement investigations or prosecutions under FOIA exemption 7(A) or 7(E), in accordance with EPA's FOIA procedures. (Note: Other potential FOIA exemptions that may affect releasing the digital images are listed at: http://www2.epa.gov/foia/learn-about-foia#exemptions.)[10] If the manager approves release after this review, the inspector must provide a copy of the digital images to a requesting facility, consistent with the FOIA, and must keep a record of the digital images that were given to a facility in EPA's inspection file. The record must identify and describe the digital images and can be noted in the field notes, on the Digital Image Log, or as a separate list. Digital images may be e-mailed using only EPA-authorized Internet connections that conform to EPA security and communications standards or shared on a website as long as the images do not contain CBI. Inspectors also may not process, store, or transmit sensitive

[10] Inspectors and managers should also be familiar with EPA's Guidance for Releasing Civil Inspection Reports, which includes expectations and other considerations for releasing information, such as digital images, that becomes part of an inspection report.

information on wireless devices unless encrypted using EPA authorized encryption methods.[11]

- Protect CBI. If a facility asks to view digital images due to CBI concerns during the inspection, the inspector may show the images only on government equipment (note prohibition above for EPA Information Security Policy). The inspector must record the images claimed to be CBI in the field notes. When taking, storing, using, or transferring digital images which contain CBI data, inspectors must follow CBI procedures set forth in 40 CFR Part 2 and in the applicable EPA CBI Manual regarding use of computers and electronic storage media at all times. In general, digital images that may contain CBI must not be sent via e-mail. Toxic Substances Control Act (TSCA) CBI may be sent via e-mail on approved Local Area Networks (LANs). Clean Air Act CBI can be sent to DOJ via DOJ's secured server (@enrd.doj.gov).
- Federal Insecticide, Fungicide, and Rodenticide Act (FIFRA) inspections. For FIFRA inspections, images must not be released until enforcement proceedings are concluded or advised by counsel in accordance with the 2013 FIFRA Inspection Manual[12].

F. Records Retention

- Working copies that are used to make decisions and all archival copies are considered records.
- For digital images that are part of compliance files only and are not part of an enforcement action, EPA Records Schedule 1044 item d states the appropriate EPA official:
  - Close (stop adding files to) the file at the end of the year (year may be the calendar or fiscal year depending on the EPA office's policies)
  - Destroy digital image records 5 years after closure.
- Copies of the compliance records incorporated into other files (e.g., site or facility files) are to be retained according to the disposition instructions for the records they support.
- Upon issuance of a notice of violation or referral to Regional Counsel or other office with enforcement authority, the digital image record becomes an enforcement action file.
- Consistent with EPA Records Schedule 1044 items a, b, or c, if a digital image enters an enforcement case file and is not Superfund or oil site-specific related, the appropriate enforcement official:
  - Close inactive digital image records upon settlement or closing of case.
  - Destroy digital image records from administrative case files 10 years after file closure (1044c).

[11] It may be possible to burn a copy of digital images taken during an inspection onto an unalterable CD or similar unalterable device before leaving an inspection site if the inspector has either been (a) delegated the authority to oversee the quality assurance and quality control of their own inspection report information in accordance with a Region's or program's SOP regarding inspection reports, or is able to share the images with their supervisor and gain the supervisor's approval to release the images prior to leaving the site, and (b) as long as the Information Security National Rules of Behavior, EPA Order 3500.1 Section (5)(c)(4) and processes described in this Guidance are adhered to.

[12] The FIFRA Inspection Manual states, "Federal inspectors, as well as state or tribal inspectors performing federal inspections, shall not release any notes, documents, reports, etc. obtained or prepared in connection with a FIFRA inspection until such time as enforcement proceedings are concluded or as advised by counsel."

    - Destroy digital image records from judicial case files 20 years after file closure (1044b).
    - Transfer digital image records from landmark or precedent cases (determined by the inspector's records office) to the National Archives 15 years after file closure (1044a).
- For Superfund and oil site-specific enforcement actions consistent with EPA Records Schedules 025 and 480 respectively (soon to be superseded by EPA Records Schedule 1036), the appropriate enforcement official:
    - Close inactive records upon settlement or closing of case
    - Destroy cases with routine legal action or no legal action required 30 years after file closure
    - Transfer digital image records from landmark cases to the National Archives 5 years after file closure
    - Close the electronic copy of records file from landmark cases transferred to the National Archives upon transfer to the National Archives and delete the digital images after the electronic record copy is successfully transferred to the National Archives
- Inspectors in possession of images subject to a litigation hold may be required to retain those images past the scheduled retention period.
- The appropriate enforcement official may only transfer images to NARA that are sound and free from defects and must comply with NARA's format requirements when preparing digital records for transfer. Acceptable formats can be found in Appendix C.

REFERENCES/ADDITIONAL INFORMATION

1. Berg, Erik, "Legal Ramifications of Digital Imaging In Law Enforcement", Forensic Science Communications, Vol 2, No. 4, October 2000, Available at http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/oct2000/berg.htm
2. California Environmental Protection Agency, "CalEPA Suggested Guidelines for Digital Photos," Rev. 12/09. Available at: http://www.calepa.ca.gov/enforcement/Policy/Photos.htm.
3. Food and Drug Administration (FDA), "Subchapter 5.3 – Evidence Development," Investigations Operations Manual. Available at: http://www.fda.gov/ICECI/Inspections/IOM/ucm122531.htm.
4. Lorraine v. Markel Am. Ins. Co. 241 F.R.D. 534, 546, 547, 561. United States District Court for the District of Maryland. 2007.
5. Microsoft, "Ensuring Data Integrity with Hash Code." Available at: http://msdn.microsoft.com/en-us/library/f9ax34y5(v=vs.110).aspx.
6. NJ Division of Criminal Justice, "A Standard Operating Procedure for Use of Digital Imaging Cameras by the First Responding Officer," Revision 3/05. Available at: http://www.nj.gov/oag/dcj/njpdresources/pdfs/digital_imaging%20_sop.pdf.
7. Rhode Island Department of Environmental Management, "Digital Photograph Record Collection and Storage SOP: SOP-OD-QM-4," Revision No. 0, August 16, 2007. Available at: http://www.dem.ri.gov/pubs/sops/photocol.pdf.
8. Scientific Working Group on Imaging Technology (SWGIT), "Best Practices for Forensic Video Analysis," Version 1.0, January 16, 2009, Final. Available at: https://www.swgit.org/pdf/Section%207%20Best%20Practices%20for%20Forensic%20Video%20Analysis?docID=51.
9. Search Storage, "WORM (write once, read many)," September 2005. Available at: http://searchstorage.techtarget.com/definition/WORM-write-once-read-many
10. State v. Swinton. 268 Conn. 781, 809. Supreme Court of Connecticut. 2004.
11. SWGIT, "Best Practices for Image Authentication," Version 1.1, January 11, 2013, Final. Available at: https://www.swgit.org/pdf/Section%2014%20Best%20Practices%20for%20Image%20Authentication?docID=39.
12. SWGIT, "Best Practices for Maintaining the Integrity of Digital Images and Digital Video," Version 1.1, January 13, 2012, Final. Available at: https://www.swgit.org/pdf/Section%2013%20Best%20Practices%20for%20Maintaining%20the%20Integrity%20of%20Digital%20Images%20and%20Digital%20Video?docID=54.
13. SWGIT, "Issues Relating to Digital Image Compression and File Formats," Version 1.1, January 15, 2011, Final. Available at: https://www.swgit.org/pdf/Section%2019%20Issues%20Relating%20to%20Digital%20Image%20Compression%20and%20File%20Formats?docID=42.
14. SWGIT, "Overview of SWGIT and the Use of Imaging Technology in the Criminal Justice System," Version 3.3, June 11, 2010, Final. Available at: https://www.swgit.org/pdf/Section%201%20Overview%20of%20SWGIT%20and%20the%20Use%20of%20Imaging%20Technology%20in%20the%20Criminal%20Justice%20System?docID=35.
15. SWGIT, "Recommendations and Guidelines for Crime Scene/Critical Incident Videography," Version 1.0, January 13, 2012, Final. Available at: https://www.swgit.org/pdf/Section%2020%20Recommendations%20and%20Guidelines%20for%20Crime%20Scene%20and%20Critical%20Incident%20Videography?docID=44.

16. United States Department of Agriculture (USDA), "Photographic Evidence Collection," September 30, 2013. Available at: http://www.fsis.usda.gov/wps/wcm/connect/6e352b7a-ab48-4bee-b078-1ad5f5dc67ad/24-Photographic-Evidence.pdf?MOD=AJPERES
17. United States v. Espinal-Almeida. 699 F.3d 588, 609. United States Court of Appeals, First Circuit. 2012.
18. United States v. Savarese, 686 F.3d 1, 10, 11. United States Court of Appeals, First Circuit. 2012.
19. United States Environmental Protection Agency (EPA), "Policy on the Use of Mobile Field Inspection Tools," June 17, 2016. Available at: https://www.epa.gov/compliance/policy-use-mobile-field-inspection-tools
20. Chastain, Sue, "JPEG Myths and Facts." Available at: http://graphicssoft.about.com/od/formatsjpeg/a/jpegmythsfacts.htm

Cover Image

Cover image courtesy of Cute Pictures.

<Organization>

Standard Operating Procedure

Capturing, Storing and Preserving Digital Images

Number: <Document Control Number>
<Date>
U.S. Environmental Protection Agency

U.S. Environmental Protection Agency <Organization> Controlled Document	
STANDARD OPERATING PROCEDURE	
Title: **Capturing, Storing and Preserving Digital Images**	
Effective Date: <DATE>	**Number:** <Document Control Number>
Author	
Name: <AUTHOR> Title: <TITLE> Office: Signature:	Date:
Approvals	
Name: <AUTHOR> Title: <TITLE> Office: Signature:	Date:
Name: <AUTHOR> Title: <TITLE> Office: Signature:	Date:
Name: <AUTHOR> Title: <TITLE> Office: Signature:	Date:
Name: <AUTHOR> Title: <TITLE> Office: Signature:	Date:
Name: <AUTHOR> Title: <TITLE> Office: Signature:	Date:

Revision History

This table shows changes to this controlled document over time. The most recent version is presented in the top row of the table. Previous versions of the document are maintained by the OECA Document Control Coordinator.

History	Effective Date
Capturing, Storing and Preserving Digital Images, original issue	<DATE>

CONTENTS

<TOC must be regenerated upon completion of SOP content. To do so, click in TOC below, select Update Field, then select Update entire table>

General

Summary of Procedure/Purpose

<Describe the intended use or purpose of controlled document>

This document describes the procedures for capturing, storing and preserving digital images for inspections / field investigations.

Scope / Applicability

<Describe scope of document – who does it apply to and when does it need to be followed>

This procedure applies to <Organization> personnel who plan or conduct on-site facility inspections and investigations. Additionally, this procedure applies to federally credentialed contractors and grantees conducting inspections / field investigations on behalf of EPA.

Individual programs or organizations may have additional requirements regarding the generation, storage or preservation of digital images beyond the procedures identified herein.

This SOP has been developed for EPA employees and is intended solely for internal management purposes. It does not create any rights, substantive or procedural, enforceable at law. EPA may periodically revise this SOP to make improvements and/or to reflect changes in EPA policy. EPA reserves the right to act at variance with this procedure.

If, on a case-by-case basis, an EPA employee chooses to vary from a provision of this SOP, such variance must be explained and documented. Varying from this procedure does not disqualify information obtained for any purpose.

Documentation / Verification

<Identify any special qualifications users should have, such as a certification, specific training and/or any individual or positions having responsibility for the activity described>

This procedure was prepared by persons deemed technically competent by the appropriate <Organization> management, based on their knowledge, skills, and abilities. The official copy of this procedure is maintained by the Document Control Coordinator (DCC), and a copy is accessible to all <Organization> staff in the <Designated Operating Procedure Location>.

Personnel Qualifications/Responsibilities

<Describe responsibilities of staff involved>

All staff who capture, store or preserve digital images for inspections/field investigations must implement this work in a manner consistent with all applicable <Organization> standard operating procedures (SOPs).

References/Other Associated Procedures

<This can include any Agency guidance/policies/procedures, associated procedures, instrument manuals, forms that should be used, etc.>

- Digital Image Guidance for EPA Civil Inspections and Field Investigations (Month, 2016)
- EPA Information Procedure: Information Security – National Rules of Behavior (CIO 2150-P-21.0)
- Policy on the Use of Mobile Field Inspection Tools (June 17, 2016)

Definitions

Definitions for certain terms included in this SOP are provided in < Specify where the Organization's SOP definitions are maintained.>

Definitions specific to this SOP include:

- **Non-Authorized Wireless Network**. A wireless network solution and configuration that is not configured in accordance with the EPA's Chief Information's Officer's technical standards and specifically authorized by the Senior Information Official.
- **Archival (Master) Copy**. An unchanged, unedited copy of the original digital images that will be used as the permanent record. It is the functional equivalent to the "negatives" in film photography.
- **Working Copy.** A "back-up" copy of the original digital images which may be used to make minor enhancements or edits such as cropping and improving contrast.

Procedure

Summary of Procedure/Method

<Describe actual steps needed to complete tasks. This is the main section of the controlled document and is likely to have several subsections. This section should be clearly worded so as to be readily understandable by a person knowledgeable with the general concept of the procedure and the procedure(s) should be written in a format that clearly describes the steps in order.>

This procedure outlines <Organization's> process to capture, store and preserve digital images. It is the responsibility of the inspector and his/her first line supervisor to ensure that all applicable Agency and program-specific requirements are satisfied. The capture and management of digital images must be conducted in accordance with applicable SOPs including Field Documentation, Field Equipment and Records Management.

Digital Devices

<Describe the digital devices that will be used>

Only EPA-approved and issued digital devices will be used to capture and store digital images. EPA-approved and issued digital devices must not:

- Be connected to a non-EPA digital device.
- Access non-authorized wireless networks.

Digital devices must always be kept in the possession of the inspector / field investigator or in a secure location during the entire inspection / investigation until it is securely transferred to another location or authorized person at the conclusion of the inspection / field investigation.

Preparing for an Inspection / Field Investigation

The Inspector / field investigator must be familiar with the digital device's features. Prior to use, the inspector / field investigator must determine that:

- The digital device is in working order and charged (including availability of back-up battery power/ digital device charger.)
- The digital device's date and time settings (where applicable) are correct and corrected if inaccurate.
- There is adequate media storage space for the digital images to be captured.

Capturing and Recording Digital Images

Inspectors / field investigators must seek to capture images that are as clear as practicable and show relevant details. All digital images, even those that are poor quality, taken inadvertently, or do not show relevant details must be maintained on the digital device until an archival copy is created (see Section 2.5). <In the rare circumstance that a digital image is deleted during an inspection (e.g., the image

inadvertently captures CBI information that is not necessary for the inspection, image inadvertently includes facility staff which conflicts with facility policy) the inspector should retake an image that avoids the concern. Inspectors must document all digital images deleted during an inspection and the reason for the deletion.>

Denial of Access

Facility restrictions on an inspector's ability to capture digital images may be considered a denial of access. <Reference Organization's relevant SOP regarding facility access *or* provide your organizations' process to address the denial:

If restrictions on digital images are considered a denial of access, immediately:

- *Cite the appropriate EPA inspection authority to the company official, ask if he/she understands the reason for your request to capture a digital image, and record the answer and any reason given for denial.*
- *Record the name, title and telephone number of the individual denying your request, as well as the date and time.*
- *Leave the premises.*
- *Document any site conditions and the events related to the denial after leaving the facility and inform your immediate supervisor and EPA Counsel.>*

Digital Image Quality

<If desired, describe procedures inspectors/field investigators should use to capture digital images>

Inspectors / field investigators should implement the following steps to capture images:

- Use the lowest level of image compression and size.
- Pair the digital camera with a GPS
- Take at least one image with the camera body perpendicular to the object with the camera's image sensor parallel to the object.
- Capture the subject from multiple angles / distances.
- Capture the image with and without a scale (e.g., penny, ruler).
- Use a time stamp on the image if the time stamp will not obscure evidence being recorded.
- View captured images in the field (if possible) to determine if the images accurately depict your observations.

Documenting Digital Images

Inspectors / field investigators must document digital images captured during an inspection / field investigation. <As needed, specify how digital images will be documented>

The following information must be captured in the photo log:

- Identity of the photographer/videographer;
- Date and time the image is captured;

- Location (e.g., facility name, 90 day storage area in back room);
- Brief description;
- Identifying number of digital image; and
- Other relevant metadata when available, and if practicable, such as shutter speed, f-number (sometimes called focal ratio, f-ratio, f-stop, or relative aperture), ISO setting, exposure, global positioning system (GPS) coordinates, etc.

Inspectors / field investigators must document in the inspection file the location of the original or archived digital images. (See Section 2.5 for more on archived digital images.)

Inspectors / field investigators must document the deletion of any digital images including the reason for the deletion. (See Section 2.3 for information.)

Digital Image Modifications

<Describe how digital image modifications will be made and documented>

Inspectors / field investigations must document modifications made to digital images in a digital image modification log. The documentation must be sufficiently detailed to enable a replicate modified digital image to be created from the original digital image. Modifications to digital images must be made on a working copy; never modify original digital images or archival copies. Inspectors / field investigators must save working copies of digital images with a file name that differs from the original digital image.

Documentation for each digital image modification must include the:

- Identity of the person making the modifications
- Date modifications are made
- Type of modifications (e.g., cropping, reducing, changing contrast)
- Reason for modification (e.g., image cropped to remove personnel in image)
- Identifying number of the digital image

Preserving Digital Images

<Describe how digital images will be preserved>

As soon as practicable after the inspection / field investigation, the inspector / field investigator must take steps to prevent alterations to the digital images.

Inspectors / field investigators must create an archival (master) copy of all original digital images taken during the inspection / field investigation as soon as practical after the digital images are captured. Archival copies must be created as read-only, password protected electronic files and stored on a secure network server or hard drive or saved on an unalterable media storage device

After archival copies of original digital images are created, digital images may be deleted from the digital device storage media and the digital device storage media may be reused.

Transferring Digital Images to EPA Issued Computer

<Describe how digital images will be transferred while preserving digital date stamps>

When transferring digital images to an EPA issued computer, inspectors / field investigators must prevent the computer from altering the digital image. An EPA-authorized Internet connection that conforms to EPA security and communications standards must be used to e-mail digital images. (See Section 2.8 for Confidential Business Information claims.)

Releasing Digital Image

<Describe how requests for digital images requested in the field and through FOIA will be handled. In any event, procedures must conform with the EPA Information Procedure: Information Security – National Rules of Behavior (CIO 2150-P-21.0) >

Inspectors / field investigators may show digital images captured during an inspection / field investigation to facility representatives.

Inspectors / field investigators must not:

- Connect their digital device to non-EPA devices to transfer digital images.
- Use a non-authorized wireless network to download or email digital images to the facility.

Facility staff may take their own digital images of the same subjects as the inspector / field investigator.

In the event a facility asks for copies of digital images captured during an inspection / field investigation, the inspector / field investigator may:

- <Advise the facility that copies of the digital images may be requested through the Freedom of Information Act (FOIA) and such requests will be processed in accordance with 40 CFR Part 2; *or*
- Seek approval from his/her first-line supervisor or <Office of Regional Counsel / Office of General Counsel> on the release of the digital images.>

Prior to releasing digital images, record the digital images which will be provided to the facility and include this record in the inspection file. This record must identify and describe the digital images. Digital images released may only be emailed to the requester using EPA-authorized Internet connections or shared on a website as long as the digital images do not contain CBI.

Protecting Confidential Business Information (CBI)

Inspectors / field investigators must document in their field notes any claim that a digital image is CBI. When taking, storing, using, or transferring digital images which contain CBI data, inspectors / field investigators must manage the digital images in accordance with 40 CFR Part 2, Subpart B, and any media specific guidance or EPA CBI procedures. All inspectors must have completed appropriate statute-specific training to be cleared to handle CBI by statute.

Including Digital Images in Inspection / Field Investigation Reports

Digital images used in inspection / field inspection reports must come from the working copy of the original digital images.

Records Retentions

Digital images captured during an inspection / field investigation must be retained in accordance with relevant EPA record schedules. (See schedules 1044 and 1036.)

APPENDIX B

Example Digital Image Log

United States Environmental Protection Agency

Digital Image Log A

1. Case Number: 12345	**2. Inspector Name:** John Doe		
3. Date of Inspection: 6/13/17	**4. Company Name:** ABC Company		
5. Street Address of Digital Images: 123 Street Name	**6. City:** Town	**7. State:** MD	**8. Zip:** 12345
9. Image Numbers: 1-3	**10. File Name (if any):** 6-13-17-ABC Company-Town-MD-archive		

Digital Image Number	Sample Number (if any)	Description of Digital Image	Date and Time Digital Image Taken
1		Wide shot of ABC facility	6/13/17 9:05 am EST
2		Medium shot of ABC facility	6/13/17 9:06 am EST
3		Close up of entrance to ABC facility	6/13/17 9:07 am EST

United States Environmental Protection Agency

Digital Image Log B

Name: John Doe **Date:** 6/13/17 **Case Number:** 12345

Image Number	Description
1	Wide shot of ABC facility
2	Medium shot of ABC facility
3	Close up of entrance to ABC facility

United States Environmental Protection Agency

Digital Image Modifications Log A

1. Case Number: 12345	**2. Modifier:** John Doe		
3. Date of Original Inspection: 6/13/17	**4. Company Name:** ABC Company		
5. Street Address of Digital Images: 123 Street Name	**6. City:** Town	**7. State:** MD	**8. Zip:** 12345
9. File Numbers: 1	**10. File Name (if any):** 6-13-17-ABC Company-Town-MD-working copy-		
11. Image Editing Program and Version: Photoshop CS6			

Modified Digital Image Number	Date Modification Made	Sample Number (if any)	Types of Modification	Description of Modifications
1	6/13/17		Sharpened, lightened, cropped	Sharpened and lightened to view drum label better. Cropped out my fingers from the frame

United States Environmental Protection Agency

Digital Image Modifications Log B

Name: John Doe **Date:** 6/13/17 **Case Number:** 12345

Image Number	Modifications Made
1	Sharpened and lightened to view drum label better. Cropped out my fingers from the frame

APPENDIX C

Requirements of the National Archives and Records Administration regarding preferred and acceptable digital video and photograph formats, as amended, are incorporated by reference.

https://www.archives.gov/records-mgmt/policy/transfer-guidance-tables.html

https://www.archives.gov/preservation/products/definitions/filetypes.html

DIGITAL VIDEO

ACCEPTABLE FORMATS:	• AVI (Audio Video Interleaved Format) • MOV (QuickTime File Format) • WMV (Windows Media Video 9 File Format) • MPEG-4:2:2 Profile, Main Level (Moving Picture Experts Group-4 Video) • MPEG-2 Main Profile, Main Level (Moving Picture Experts Group-2 Video) • MXF (Material Exchange Format)

DIGITAL PHOTOGRAPHS

PREFERRED FORMATS:	• TIF/TIFF (Tagged Image File Format)
ACCEPTABLE FORMATS:	• JPG/JPEG/JFIF (Joint Photographic Experts Group / JPEG File Interchange Format) • DNG (Digital Negative) • PNG (Portable Network Graphics) • JP2 (Jpeg2000) • PDF (Portable Document Format)