

UNITED STATES DEPARTMENT OF AGRICULTURE
FOOD SAFETY AND INSPECTION SERVICE
WASHINGTON, DC

FSIS DIRECTIVE

8010.3
Rev. 5

5/23/17

PROCEDURES FOR EVIDENCE COLLECTION, SAFEGUARDING AND DISPOSAL

CHAPTER I - GENERAL

I. PURPOSE

This directive provides the methodologies that FSIS personnel in the Office of Investigation, Enforcement, and Audit (OIEA), Compliance and Investigations Division (CID); Office of Field Operations (OFO), District Offices; Office of Public Health Science (OPHS), Regulatory Field Service Laboratories; Office of the Administrator (OA), Internal Controls Staff (ICS); and other authorized program employees (collectively referred to as "program employees") are to apply when collecting, safeguarding, and disposing of evidence in the performance of surveillance, investigations, and other activities under the Federal Meat Inspection Act (FMIA), the Poultry Products Inspection Act (PPIA), the Egg Products Inspection Act (EPIA), the Humane Methods of Slaughter Act (HMSA), and related laws and regulations (collectively referred to as "the Acts"). FSIS is reissuing this directive in its entirety to provide additional information related to photography collection and authority, using smartphones to collect evidence, collecting investigative samples using the Public Health Information System (PHIS), and to make other clarifications.

KEY POINTS:

- *Three general categories of evidence.*
- *Procedures for collecting, safeguarding, and disposal of evidence, including photographs and videos.*
- *Procedures for using government-issued smartphones for evidence collection.*
- *Procedures for collecting investigative samples using PHIS.*
- *Procedures for transferring and receiving evidence.*
- *Procedures for retention and disposal of evidence.*

II. CANCELLATION

FSIS Directive 8010.3, Revision 4, Procedures for Evidence Collection, Safeguarding, and Disposal, 4/24/14.

III. FSIS FORMS ASSOCIATED WITH THIS DIRECTIVE

A. The following FSIS forms are located at:

<https://inside.fsis.usda.gov/fsis/emp/static/global/forms/forms.jsp>. Users need to have e-Authentication to access the site.

FSIS Form 8000-7B (Photographic Report) - provides a detailed description of the subject of the photograph, the location where the photograph was taken, the date the photograph was taken, and the name of the photographer.

FSIS Form 8000-15 (Photographic Log) - Section I identifies the subject or location photographed; Section II identifies the type of media and a specific description of each photograph; and Section III provides for a reference sketch of the area/items photographed.

FSIS Form 8050-2 (Shipper's or Receiver's Certification) - may be used when initial contact is made with the shipper or receiver of meat, poultry, egg products, or shell eggs that appear to be in violation of the Acts.

FSIS Form 8200-1 (Property Receipt) - is completed when an original or source document is presented by the owner or custodian of records, documents, or other items of personal property when that property is collected as evidence. The original form is used to authenticate the documents and is signed by the investigator and owner or custodian of the source documents. The original form is maintained with the case file and a copy is provided to the owner or custodian.

B. The FSIS Forms identified below are completed in the AssuranceNet/In-Commerce System (ANet/ICS). For program employees who do not have access to ANet/ICS, the above forms are available at <https://inside.fsis.usda.gov/fsis/emp/static/global/forms/forms.jsp>.

FSIS Form 8000-16 (Evidence Log) - provides a detailed accounting of all evidentiary items collected in an investigation and is used to monitor the control and accountability of these items.

FSIS Form 8000-17 (Evidence Receipt and Chain of Custody) - Section I identifies the evidentiary items collected in an investigation and establishes the chain of custody for that evidence; Section II tracks the chain of custody to maintain control and accountability for the items; and Section III documents the final disposal action of the items.

IV. BACKGROUND

A. OIEA/CID Investigators, Senior Investigators (Srl), Supervisory Investigators (SI), and Regional Directors (RD) conduct surveillance, investigations, and other activities; OA/ICS Personnel Misconduct Investigators (PMI) conduct misconduct investigations and other activities; OFO Enforcement, Investigations, and Analysis Officer (EIAO), Supervisory EIAO (SEIAO), District Case Specialist (DCS), Deputy District Manager (DDM), and District Manager (DM) conduct regulatory investigations, Food Safety Assessments (FSA), and other activities; and OPHS Field Service Regulatory Laboratories conduct scientific testing to aid in the detection and prevention of foodborne illness outbreaks, support investigations, and other activities.

B. The evidence collected and safeguarded during these activities is essential to the Agency mission and to support Agency decisions, regulatory action, investigative findings, and enforcement or other legal actions. Evidence includes documents, photographs, investigative samples, items, and other facts or records collected during surveillance, investigations, FSAs, and other activities.

C. The safeguarding of evidence includes the steps needed to establish legal integrity (i.e., identification, security, handling, and chain of custody) from the time of initial acquisition to final disposal. These steps prevent loss, unauthorized alteration, mishandling, or other actions that may

affect the integrity of evidence. Chain of custody is the methodology used to maintain, track, and document control of all evidentiary items. Chain of custody includes the order of places where, and the persons with whom, evidence collected by FSIS program employees was located from the time it was collected to its disposal. Failure to safeguard evidence may affect the use of that evidence to support enforcement or legal actions. Evidence disposal addresses retention, disposal requirements, and procedures.

D. Other authorized Agency personnel may sometimes collect evidence while performing official duties and are to follow the procedures set out in this directive to collect, safeguard, and maintain evidence.

CHAPTER II - EVIDENCE COLLECTION

I. GENERAL

A. Evidence may be used to support Agency decisions, to support that a violation of law has occurred, to take enforcement actions, to help obtain a ruling in a court of law, or to accomplish other purposes. When collecting evidence, program employees are to treat every item of evidence in the manner described in this directive. The proper treatment and the preservation of evidence in the condition in which it was collected require that all authorized persons handle evidentiary items with care. Establishing and maintaining a chain of custody for all evidence collected is of utmost importance to provide for accountability for, and for maintaining a record of, the conditions under which the items were held at each stage of evidence collection, safeguarding, and disposal.

B. There are three general categories of evidence for which the procedures outlined in this directive apply. These categories are:

1. Documentary evidence (may also be referred to as physical evidence);
2. Photographic evidence (may also be referred to as digital evidence); and
3. Investigative samples.

C. Program employees may, as necessary, develop demonstrative exhibits to illustrate, clarify, or summarize evidence (i.e., documents, records, items, photographs, or samples) collected during surveillance, investigations, FSAs, and other activities. Demonstrative exhibits need to fairly and accurately represent the evidence. Examples of demonstrative exhibits include diagrams, flowcharts, maps, drawings, or graphs. Program employees are to include any demonstrative exhibits in the list of exhibits. Because demonstrative exhibits are generated by the program employee, and not collected from a subject or witness of an investigation, it is not necessary to prepare FSIS Form 8000-17, the Evidence Receipt and Chain of Custody form.

D. When evidence is obtained as digital files (e.g., scanned document files, files obtained via e-mail from a firm, video, data spreadsheet), program employees are to follow the instructions in the Photographic Evidence section below to identify and maintain the digital evidence on a CD-R with an Evidence Receipt and Chain of Custody form. A DVD-R (or larger government-issued digital device) may be used to maintain digital evidence files that are larger than 700 MB.

II. DOCUMENTARY EVIDENCE

A. Documentary evidence is the most common form of evidence collected by FSIS during investigations and other activities. Documents, including various forms of statements collected by program employees during surveillance, investigation, and other activities, may be used to support Agency decisions, enforcement actions, and investigative findings or to support legal action in

Federal, state, or local court.

B. It is imperative that a government witness (usually the person who collected the record) be able to testify as to where, when, and from whom the documents were collected and to the fact that the copy is a true and correct copy of the source document, based on his/her review of the source document.

C. Documentary evidence is a type of evidence that is in physical form rather than oral form, including writings on paper as well as physical forms of media that are collected from a subject or witness.

D. Examples of documentary evidence include:

1. Sales invoices (as a means of identifying the seller or buyer; the amount, type, price, or date of the sale; or purchase or receipt of the product);
2. Receiving and storage records (as a means of identifying dates relevant to product storage, product condition or temperature, or storage temperature);
3. Product labels (the physical, printed label; if obtained as a photograph it is digital/photographic evidence);
4. Transportation records (as a means of identifying the transporter, the location the product was shipped from, or the location to which the product was shipped);
5. Rodent and pest control service records;
6. Contracts, Agreements, or similar transactional documents;
7. E-mails received from firm or individual (when proffered);
8. Sanitation Standard Operating Procedures (Sanitation SOP) records and Hazard Analysis Critical Control Point (HACCP) records;
9. Production records (e.g., establishment production dates, lot numbers, pre-shipment review conducted);
10. Laboratory analysis records of product (analysis requested by a manufacturer, custodian, or owner);
11. Records or reports documented by Federal, State, or local authorities of noncompliance, violations, or other issues (e.g., FSIS Form 5400-5 Establishment/Shift Inspection Procedure Worksheet, FSIS Form 5400-4 Noncompliance Record);
12. Statements (signed and unsigned) documenting an interview;
13. Memorandums of Interview (MOI);
14. Diagrams, maps, charts, or graphs collected from a subject or witness during an investigation; and
15. Photographic prints, videos, or other items collected from a subject or witness during an investigation as a physical copy (e.g., printed material, government-issued flash drive, audio/video DVD/CD/tape/external device).

E. To collect documentary evidence, program employees are to use the following procedures:

1. Make a request to a responsible official to examine records, documents, or items;
2. Examine and determine the specific records to collect; and
3. Collect appropriate records, documents, or items:
 - a. Copies – Obtain selected documentary evidence by requesting copies or the opportunity to make copies, scan, or photograph each individual record or document or item.
 - b. Original – Obtain the source document if a copy is not available (see Section G. 3).

F. The Acts provide FSIS personnel authority to examine facilities, inventory, and records at federally inspected establishments and at warehouses, distribution centers, and other in-commerce facilities subject to the statutes (21 U.S.C. 455, 460, 609, 642, 1034, and 1040). These statutory provisions provide duly-authorized representatives of the Secretary with access to the place of business; with an opportunity to examine the facilities, inventory, and records thereof; and with an opportunity to copy all such records. If necessary, contact the Enforcement and Litigation Division (ELD), OIEA, through supervisory channels to request an administrative subpoena to access the facility or to collect copies of records. See [FSIS Directive 8010.5](#), *Case Referral and Disposition*.

G. To identify documentary evidence, program employees are to:

1. Complete Section I of an Evidence Receipt and Chain of Custody form in ANet/ICS by completing the appropriate data fields, print a hard copy and sign it, and maintain the hard copy with the original evidence in a secure location;

NOTE: Official FSIS forms or Agency investigative or administrative reports (e.g., FSIS Form 8080-1, Notice of Detention; FSIS Form 8000-7, Exhibit Cover Sheet; FSAs) are not to be initialed or dated.

2. Initial and date the back of each document or record that is obtained as a copy collected (e.g., initials mm/dd/yy). There are occasions when a single piece of documentary evidence may consist of hundreds of sheets of paper, which may or may not be bound or sequentially numbered (e.g., page 6 of 10). In these instances, program employees may use an abbreviated method to initial and date these documents. If the program employee ensures that all pages are accounted for, the program employee may initial and date the first and last page and identify the number of pages (e.g., page 1 of 500 on the first sheet and page 500 of 500 on the last sheet);
3. Issue a Property Receipt to the owner or custodian when a source record, document, or item, is obtained *in lieu* of a copy. Source documents are considered personal property. As such, the program employee is to maintain the Property Receipt with the case file. Personal property is to be returned to the owner or custodian in the same condition as received; therefore, program employees are to ensure these records, documents, or items are not altered in any way. The Property Receipt is to be completed and a copy given to the owner or custodian to ensure that these records, documents, or items are identified and authenticated; and
4. Sign and date each statement or MOI.

III. PHOTOGRAPHIC EVIDENCE

A. Photographic evidence is one of the most effective and useful forms of evidence. Photographic evidence, which includes digital photographs, including video (when appropriate and in consultation with supervisors), provides visual evidence to establish violative conditions or products, insanitary conditions or practices that are likely to render products injurious to health, or other observations. Photographs provide a means to visually bring the facility or location to the decision-maker to support Agency decisions, enforcement actions, and investigative findings. Photographs also may be used to record business and other documents, when necessary or efficient, in place of collecting or reproducing copies.

B. Photographic evidence is a type of evidence that uses photography or videography to capture images of conditions, products, practices, observations, and other visualizations; this evidence is collected by program employees.

C. Examples of conditions or practices effectively documented by photographic evidence include:

1. Evidence of rodents, insect infestation, other insanitary conditions, or facility construction or maintenance problems that contribute to insanitary conditions;
2. Routes of, as well as actual contamination of, raw materials or finished products;
3. Condition of raw materials or finished products;
4. Product labels, other labeling, invoices, or other documents, including digital files from scanning;
5. Insanitary conditions or equipment contributing to contamination or to violative condition of raw materials or finished products;
6. Employee practices contributing to contamination or to violative condition of raw materials or finished products; and
7. In-commerce forms or official establishment records, including records showing errors; substitutions; penciled changes in procedure; faulty practices; deviations from HACCP; Sanitation SOP; other prerequisite programs; other protocols; altered or inadequate control procedures; or other deviations from a stated procedure.

D. The FMIA, PPIA, and EPIA provide FSIS personnel broad authority to conduct inspections and examinations of the premises, facilities, inventory, records, equipment, and operations of federally inspected establishments, warehouses, distribution centers, and other in-commerce facilities subject to the statutes (21 U.S.C. 455, 460, 604, 609, 642, 1034, and 1040). These statutory provisions also provide program employees authority to copy certain business records. Program employees are to use photography, under these authorities, as a technique to examine facilities, equipment, operations, inventory, records, and where necessary to copy business records. Permission from company management to take photographic evidence during surveillance, investigations, or other activities is not necessary.

1. When facility personnel or officials refuse to allow program employees to take photographic evidence, program employees are to explain the statutory authority cited above, and that the camera is a tool used in the examination of facilities and inventories and for copying business records. Refusal to allow program employees to take photographic evidence under these authorities in an official establishment may be considered interference with inspection, subject to withholding action or suspension without prior notification in accordance with 9 CFR 500.3(a)(6). If necessary, contact ELD through supervisory channels to request an administrative subpoena; and

2. Program employees are not to surrender cameras, film, digital images, or photographs to facility personnel or officials. Program employees are to advise the establishment that it can seek to obtain copies of the photographs under the Freedom of Information Act (FOIA).

E. Program employees are to use government-issued digital or smartphone cameras, or, when necessary, film-based or other photographic equipment, to collect photographic evidence. To collect photographic evidence on a government-issued camera or smartphone, program employees are to use the following procedures:

1. Capture the scene in a comprehensive, logical sequence whenever possible. The sequence should provide an overview of the entire area, a medium eye-view angle, close-up, and extreme close-up images of the subject. Avoid deleting any images in the sequence, even if poorly exposed;
2. Prevent the disturbance of the scene until the necessary images are collected. Once the images have been taken, the investigation or other activity may continue;
3. Ensure conclusive photographic or videographic identification of the location, as appropriate, in both the exterior and interior sections of the facility (e.g., include an identifiable landmark, such as a street sign, in a photograph of the exterior of the facility); and
4. When it is important to depict scale of the subject of a photograph/video, use a ruler or similar item strategically placed in the close-up images of the subject.

F. To collect photographic evidence, which includes photographs and videos, on a government-issued smartphone, program employees are to use the following procedures:

1. Before using the smartphone for photographic evidence collection, ensure all external photo-sharing options are turned off (including turning off iCloud Photo Library (iPhone), Auto Backup (Android), and any other auto-syncing applications);

NOTE: Personal (non-government) smartphones are not to be used to collect evidence. Program employees are not to download personal-use, social media, or networking applications to their government-issued smartphones. Program employees are not to text, share, or modify photos on cameras or smartphone applications ([FSIS Directive 1306.18](#), *Safeguarding Mobile or Portable Electronic Equipment and Data*).

2. Transfer the photographs/videos to a CD-R or DVD-R as soon as practical as set out in section G below; and
3. Promptly delete the photographs/videos from the smartphone after successful transfer of the photographs to the CD-R is verified.

G. To identify photographic evidence, program employees are to:

1. Initiate and maintain a Photographic Log to identify the subject or location being photographed and include a description of each photograph;
 - a. A single entry in the Photograph Log may be used to describe a series of photographs that depict a situation or conditions if the entry is sufficient to describe what is being depicted (e.g., 00011 – 00020 show insanitary conditions in cooler B at XYZ Company);

- b. When information relevant to photographs of a subject or location is initially captured in investigative notes, ensure that all pertinent information is transferred into Sections I and II of the Photographic Log; and
- c. Section III of the Photographic Log may include a sketch of the subject or location being photographed. A sketch is a rough approximation of the scene that places items and locations in perspective to each other to supplement photographs.

NOTE: Under most circumstances, the Investigator is to complete a Photographic Log. Program employees, in consultation with supervisors, may determine that it is not necessary to complete a Photographic Log when, during surveillance, investigative, or other activities, a small number of photographs are taken and all are included in the final investigative report on FSIS Form 8000-7B, Photographic Report. In these cases, the Photographic Report and Evidence Receipt and Chain of Custody will serve to identify those photographs and a Photographic Log is not required.

2. Create and authenticate a master original copy of the digital photographs from a government-issued camera or smartphone as soon as practical by following these steps:
 - a. Transferring the files to a single use CD-R or DVD-R to ensure that the files cannot be modified;
 - b. Use a USB cord to connect the government-issued camera or smartphone to a government-issued computer, or directly insert the camera or smartphone's external memory card (optional smartphone accessory) into the computer's card reader, to download the files to burn to a CD-R;
 - c. Label the master CD-R by using a compatible permanent marker that will not damage the CD-R with the investigation file number, Administrative Enforcement Report (AER) report number, or other file identifier; the firm name; date; description of the subject matter; and the photographer's initials; and
 - d. Complete Section I of an Evidence Receipt and Chain of Custody form in the ANet/ICS by completing the appropriate data fields, printing a hard copy, and maintaining it with the original master CD-R.
3. Maintain the master CD-R under security as original evidence and make separate working copies, as necessary, on a computer hard drive, a CD, or other storage media for examination, printing, or enhancement.

IV. INVESTIGATIVE SAMPLES

A. Investigative samples are samples that are collected by CID Investigators as evidence to support a violation, usually during the course of a criminal investigation. Investigative sample collection is an important component of evidence collection. It includes the sampling of inventory from persons or firms engaged in preparation, distribution, or storage of meat, poultry, shell egg, or egg products. It also includes collection and analysis of other materials, as necessary. The FMIA (21 U.S.C. 642) and PPIA (21 U.S.C. 460) provide authority that includes the sampling of inventory, upon payment of fair market value, from persons or firms engaged in the preparation, distribution, or storage of meat and poultry. The EPIA contains similar authority (21 U.S.C. 1034). When samples are collected, CID Investigators need to collect and submit samples for laboratory analysis in a manner that safeguards the integrity of the evidentiary material, so that it is reliable as evidence.

B. Investigative samples are a type of evidence that requires collection of products, substances, debris, trace matter, or unidentified material for scientific testing to determine characteristics of the collected item; these characteristics may include species identification, microbiological determinations, fecal identification, chemical analysis, residue testing, and many others.

NOTE: Only CID personnel collect investigative samples as described in this directive. However, program employees (e.g., EIAOs, CID Investigators) also collect routine verification or surveillance samples (e.g., Intensified Verification Testing (IVT), retail ground beef) from persons or firms, including federal establishments, engaged in preparation or storage of meat, poultry, or egg products. Program employees are to follow the guidance in the appropriate directive or notice when they collect, prepare, and submit these samples. When OFO personnel believe a criminal investigation is needed, including the collection of investigative samples, they should immediately refer the information to CID in accordance with [FSIS Directive 8010.5](#).

C. When facility personnel or officials refuse to allow CID Investigators to obtain samples of inventory, CID Investigators are to explain the statutory authority cited above, and that reasonable samples of the inventory can be taken upon payment of fair market value. If necessary, contact ELD through supervisory channels to request an administrative subpoena.

D. FSIS OPHS has three Regulatory Field Service Laboratories – the Eastern, Midwestern, and Western laboratories. The Eastern Laboratory receives the majority of the investigative samples submitted by CID for analysis. Each FSIS laboratory has multiple disciplines, such as Chemistry, Microbiology, or Pathology. Therefore, it is essential that CID Investigators submit investigative samples to the appropriate laboratory for the requested analyses. The laboratory contact information is detailed in paragraph Q.

E. During the development of an Investigative Plan ([FSIS Directive 8010.2](#), *Investigative Methodology*) and prior to submitting investigative samples, CID Investigators are to contact the laboratory to discuss the specific analytical capabilities needed for each sample and determine the appropriate laboratory to submit their investigative samples. When the laboratory determines which laboratory should conduct the required analyses, CID Investigators are to make contact with that laboratory. If OIEA or OPHS personnel need assistance in determining the most appropriate tests, choosing samples to collect, or the relative scientific value of testing results, they are to contact OPHS (Science Staff, Applied Epidemiology Staff, or laboratory supervisor; see paragraph Q below).

F. When sample results involve potential public health issues, they are of high priority for FSIS. To ensure the appropriate submission of investigative samples and the timely reporting of significant results relevant to public health, CID Investigators are to discuss submissions with laboratory personnel before submitting samples.

G. The two primary factors in determining how quickly sample results are reported are asking the right questions prior to submitting the samples and submitting the samples correctly. Contacting the appropriate laboratory will help to ensure that:

1. The laboratory can analyze the samples for the desired analyses; and
2. The laboratory is prepared for the samples and a point of contact is made.

H. Once the CID Investigator contacts the appropriate laboratory (see paragraph Q below), he or she is to discuss with OPHS lab supervisor and Science Staff which analyses might be the most appropriate to request and how to best submit samples for those analyses. To get guidance on how best to submit each of the samples, the CID Investigator is to ask questions such as:

1. What type of sample should be submitted for a multiple analyses request and how much sample is required?
2. How many samples should be submitted for a multiple analyses request?
3. What is the best way to collect and submit each sample for a multiple analyses request?
4. What is the best way to submit each sample to facilitate the quickest possible reporting (see paragraph L below) of high priority lab results?
5. Which analyses may be incompatible with other analyses? and
6. What is the best way to ensure that results involving food safety are available as soon as possible and reported independently of other results if a sample is undergoing several analyses?

I. When CID Investigators request multiple analyses involving multiple lab disciplines, they are to submit a single sample per laboratory discipline or per analysis requested, as discussed with OPHS laboratory supervisors and Science Staff. This amount is necessary to ensure potential public health related results can be reported independently and before results of economic significance.

J. Examples of items that may be collected for analysis are:

1. Raw, in-process, or finished meat, poultry, egg products, or shell eggs;
2. Ingredients used in raw, in-process, or finished meat, poultry, or egg products;
3. Product packaging;
4. Rodent excreta, insects, apparent nesting, or vermin-gnawed material; or
5. Extraneous materials.

NOTE: When investigative sample collection is related to foodborne illness investigations, CID Investigators are to follow the product sampling guidance in [FSIS Directive 8080.3, Foodborne Illness Investigations](#), Section VIII, including inter-program area notifications and coordination as described in Section VII.

K. Sample Types

1. Intact sampling: Obtain a sample of an unopened packaged product. Collecting intact samples, if possible, is preferred; however, if intact sampling is not possible, non-intact samples may be collected.
2. Non-intact sampling: At times, intact sampling may not be practical because of the volume of product involved or the product's unpackaged state.

L. Sample Selection

1. CID Investigators are to submit one sample per each type of analysis they request.

NOTE: CID Investigators are to work with OPHS personnel to determine what test and how many tests can be performed if they only have a single sample available for testing.

2. Samples collected for laboratory analysis are to be collected from the location where the violative condition of the product is known or suspected to exist. Select the portions that will demonstrate the violative nature of the product.
3. There may be times when additional sampling is necessary to gain information or otherwise protect public health. In these situations, obtain guidance from an appropriate source (e.g., OPHS and the Office of Policy and Program Development (OPPD)) in regards to specific techniques, sampling plans, and policy.
4. If intact sampling is not feasible, non-intact samples are to be collected from bulk.
5. CID Investigators are to maintain the integrity of the sample and not cause contamination during sampling. If microbiological analyses will be requested, CID Investigators are to use aseptic techniques as outlined in [FSIS Directive 10,230.2, Procedures for Collecting and Submitting Domestic Samples for Microbiological Analysis](#), when collecting samples from non-intact samples (opened package), and to the extent necessary when collecting samples from intact (unopened package).

M. To request laboratory analysis of investigative samples, CID Investigators are to:

1. Complete PHIS form 8010-1 under the Project Code COMPLIAN;

NOTE: When PHIS is not accessible at the time of sample collection, Investigators are to complete FSIS Form 10,000-2, Domestic Laboratory Report, or FSIS Form 10,600-1, Domestic Chemical Lab Analysis, which are available from the Material Management Service Center, at <https://www.bsc.usda.gov/>, utilizing the current supply requisition procedures. CID Investigators are to denote “STC-39 Investigative Sample” in red text at the top of the form to preclude the sample from being routinely discarded if it does not meet quality standards upon receipt. In addition, the applicable Region Code is to be included on the form: OIEA Region Codes are “W” Western, “SW” Southwest, “SE” Southeast, and “NE” Northeast.

2. Provide the producer's name, address, and establishment number;
3. Provide a sample description, list of ingredients, and product codes (e.g., “sell by dates”);
4. Provide a name and address of the location where the sample was collected;
5. Provide date, time, and quantity collected;
6. Describe how the sample is identified and sealed (e.g., “sealed by____, on ____ (date, time), sealed with FSIS seal #____”);
7. Provide the e-mail contact information of the appropriate RD for transmission of sample results; and
8. Describe the analysis requested.

NOTE: If PHIS is not accessible at the time of sample collection, the laboratory will enter the results on the form, scan the form into a PDF, and e-mail it to the CID Investigator and RD. The original form will reside at the laboratory pending notification of sample disposal from the RD or designee (Section P).

N. To identify investigative samples, CID Investigators are to:

1. Photograph the product or other evidentiary material before and after sample collection, including identifying coding or labeling on the sample package;
2. Obtain identifying information (e.g., invoices, labels, or other product identification);
3. As appropriate, document a signed statement, MOI, or Shipper's or Receiver's Certification from witnesses with direct knowledge of the sample identity;
4. Complete Section I of an Evidence Receipt and Chain of Custody form in ANet/ICS by completing the appropriate data fields. Include a description of the sample/evidence, the sample serial number, print a hard copy of the form, and place the associated bar-coded, pressure-sensitive sticker from FSIS Form 7355-2B, in the appropriate block; and
5. Maintain all other identifying information (e.g., invoice, bill of lading) under separate Evidence Receipt and Chain of Custody form with the associated case file.

O. Prior to transferring investigative samples to the FSIS laboratory, CID Investigators are to:

1. Complete the first entry in Section II of an Evidence Receipt and Chain of Custody form to initiate chain of custody;
2. Maintain a copy of the signed Receipt with the associated case file;
3. Place the signed Evidence Receipt and Chain of Custody form in the package with the investigative sample;
4. Seal the sample in accordance with [FSIS Directive 7355.1](#), *Use of Sample Seals for Laboratory Samples and Other Applications*; and
5. Transfer the evidentiary investigative sample to the laboratory.

P. Final disposition and disposal of samples:

1. Because of the possibility of litigation, FSIS laboratories hold a portion of all investigative samples until notified that the sample may be discarded.
2. The RD or designee is to notify the appropriate laboratory when it is no longer necessary to hold a sample (based on consideration of the retention schedule in this directive). The notification to the laboratory needs to include the file number and associated sample serial numbers.
3. The FSIS laboratory will dispose of the samples and complete Section III of the Evidence Receipt and Chain of Custody form in accordance with this directive.
4. The FSIS laboratory will then forward the completed Evidence Receipt and Chain of Custody form to the RD or designee who requested the disposal.

Q. Laboratory contact information for inquiries:

1. OPHS Science Staff and Applied Epidemiology Staff E-mail: [FSIS – OPHS Investigations \(OPHSInvestigations@fsis.usda.gov\)](mailto:FSIS-OPHSInvestigations@fsis.usda.gov)
2. Eastern Laboratory

- a. Inquiry E-mail: [FSIS - Laboratory Inquiry - Eastern Lab \(LaboratoryInquiryEasternLab@fsis.usda.gov\)](mailto:LaboratoryInquiryEasternLab@fsis.usda.gov)
 - b. Phone: 706-546-3576
 - c. Supplies E-mail: [FSIS - Sampling Supplies - Eastern Lab \(SamplingSupplies-EasternLab@fsis.usda.gov\)](mailto:SamplingSupplies-EasternLab@fsis.usda.gov)
3. Western Laboratory
- a. Inquiry E-mail: [FSIS - Laboratory Inquiry - Western Lab \(LaboratoryInquiryWesternLab@fsis.usda.gov\)](mailto:LaboratoryInquiryWesternLab@fsis.usda.gov)
 - b. Phone: 510-814-3000
 - c. Supplies E-mail: [FSIS - Sampling Supplies - Western Lab \(SamplingSupplies-WesternLab@fsis.usda.gov\)](mailto:SamplingSupplies-WesternLab@fsis.usda.gov)
4. Midwestern Laboratory
- a. Inquiry E-mail: [FSIS - Laboratory Inquiry - Midwestern Lab \(LaboratoryInquiryMidwesternLab@fsis.usda.gov\)](mailto:LaboratoryInquiryMidwesternLab@fsis.usda.gov)
 - b. Phone: 314-263-2680
 - c. Supplies E-mail: [FSIS - Sampling Supplies - Midwestern Lab \(SamplingSupplies-MidwesternLab@fsis.usda.gov\)](mailto:SamplingSupplies-MidwesternLab@fsis.usda.gov)

CHAPTER III – SAFEGUARDING, TRANSFERRING, RETAINING, AND DISPOSING OF EVIDENCE

I. SAFEGUARDING EVIDENCE

A. Evidence is to be maintained under security and have a documented and continuous chain of custody showing the order of the places where, and the persons with whom, evidence collected was located, from the time of collection until the time it is admitted into court, or the case is resolved, and the evidence is no longer needed.

B. Evidence security is to be initiated and maintained as follows:

1. Review the pre-populated Evidence Log in ANet/ICS for each case to maintain evidence inventories;
2. Print a hard copy of the Evidence Log from ANet/ICS to file with the evidence when the case is complete, or otherwise as necessary, to monitor the control and accountability of evidence for each case;
3. Keep the number of people involved in handling evidence to a minimum (e.g., persons associated with the investigation); and

NOTE: OFO program management has determined that it will not use the Evidence Log to maintain inventories or to monitor the control and accountability of evidence. All evidence collected by OFO program employees is included in the List of Exhibits in the AER ([FSIS Directive 5100.3](#), *Administrative Enforcement Reporting (AER) System*).

5. Secure and maintain evidence in a secure, controlled-access area (e.g., a locked room, a locked steel file cabinet, or other suitably-locked enclosure), accessible only to designated personnel.

C. Chain of custody is to be initiated and maintained as follows:

1. Ensure that the transfer of evidence from one person to another is documented in Section II of the Evidence Receipt and Chain of Custody form;
2. Ensure that evidence is always accompanied with a signed, hard copy Evidence Receipt and Chain of Custody form to provide identification and the continuous chain of custody; and
3. Ensure that the Evidence Receipt and Chain of Custody form is filled out in a legible manner and signed with permanent ink.

II. TRANSFERRING AND RECEIVING EVIDENCE

A. Transferring Evidence

1. To preserve the chain of custody when evidence is transferred in person, program employees are to:
 - a. Sign Section II of the Evidence Receipt and Chain of Custody form as the person releasing the evidence and identify the purpose of the change in custody; and
 - b. Sign the evidence when received.
2. To preserve the chain of custody when evidence is transferred using the Agency-approved service for express and ground delivery or using Registered Mail, program employees are to:
 - a. Sign Section II of the Evidence Receipt and Chain of Custody form as the person releasing the evidence and identify the purpose of the change in custody;
 - b. Enclose the evidence and Evidence Receipt and Chain of Custody form in a suitable envelope or container marked to show that the contents are evidence, and that it is to be opened only by the identified recipient;
 - c. Seal the envelope or container, write the word "Sealed" on the outside of the envelope or container, and initial and date the envelope or container;
 - d. Prepare a transmittal letter or memorandum to include date, file number, description of the evidence, method of transportation, and tracking number;
 - e. E-mail or fax a copy of the transmittal letter or memorandum separately to the recipient to advise them of the transfer, except for investigative samples, as the sample analysis request PHIS form and the official sample seal serve this purpose;
 - f. Place the sealed envelope or container and transmittal letter in a larger envelope or container addressed to the recipient;
 - g. Use the Agency-approved service for express and ground delivery to transfer evidence when possible and always request tracking and signature confirmation;
 - h. Print a tracking receipt from the Agency-approved service's website and maintain with the evidence; and

- i. If Certified Mail is used, always request a Return Receipt for signature confirmation.

B. Receiving Evidence

1. To preserve the chain of custody when evidence is received in person program employees are to:
 - a. Sign Section II of the Evidence Receipt and Chain of Custody form as the person receiving the evidence; and
 - b. Maintain the signed Evidence Receipt and Chain of Custody form under security with the evidence.
2. To preserve the chain of custody as the receiver when evidence is received using the Agency-approved service for express and ground delivery or using Certified Mail, program employees are to:
 - a. Sign Section II of the Evidence Receipt and Chain of Custody form, as the person receiving the evidence;
 - b. Write the word "Opened," the initials of the employee who opened the envelope or container, and the date the envelope or container is opened on the inner envelope or container; and
 - c. Maintain the original initialed envelope or shipping package with the original evidence to provide proof of the chain of custody.

III. RETENTION AND DISPOSAL OF EVIDENCE

A. Retention schedules for evidence collected in the performance of surveillance, investigations, FSAs, enforcement actions, or other activities, are as follows:

1. General correspondence and other records:
 - a. Pertaining to surveillance activities or allegations that do not result in an investigation – destroy three (3) years after the end of the fiscal year in which the records were created;
 - b. Pertaining to product detentions that do not result in an investigation – destroy three (3) years after the end of the fiscal year in which the records were created; and
 - c. Pertaining to administrative activities (e.g., FSAs), or allegations that do not result in an investigation – destroy three (3) years after the end of the fiscal year in which the records were created.
2. Administrative case files, including Report of Investigation, Administrative Enforcement Report, associated case correspondence, and other records that result in:
 - a. Administrative Consent Order, Administrative Exempt Settlement Agreement, Administrative Judicial Decision & Order, Administrative Exempt Ineligibility Order, or voluntary withdrawal – destroy three (3) years after the end of the fiscal year in which the administrative action terminates;

- b. Notice of Warning (NOW), Letter of Information (LOI), Letter of Warning (LOW), Notice of Prohibited Activity (NoPA), or no action – destroy three (3) years after the end of the fiscal year in which the case was closed; and
 - c. A firm placed under Recordkeeping Requirements ((9 CFR 303.1(d)) – destroy three (3) years after the end of the fiscal year in which the termination notice is issued.
- 3. Criminal Case Files, including Reports of Investigation, associated evidence and case correspondence, and other records that result in:
 - a. Prosecute and result in a Conviction – destroy ten (10) years after the end of the fiscal year in which the case is closed;
 - b. Criminal case, other than the above – destroy five (5) years after the end of the fiscal year in which the case is closed;
 - c. Pretrial Diversion or other type of Agreement entered by Department of Justice – destroy three (3) years after the end of the fiscal year in which the Agreement terminates; and
 - d. Notice of Warning (NOW), Letter of Information (LOI), or no action – destroy three (3) years after the end of the fiscal year in which the case was closed.
- 4. Civil Case Files, including Reports of Investigation and associated case correspondence and other records that result in:
 - a. Civil Consent Decree, Civil Judgment, or Civil Decree of Forfeiture – destroy three (3) years after the end of the fiscal year in which the civil action terminates; and
 - b. Civil outcomes other than those listed above – destroy three (3) years after the end of the fiscal year in which the case was closed.
- 5. Other investigative reports that result in an Other type of disposition or that are closed with No Action – destroy three (3) years after the end of the fiscal year in which the Other disposition terminates or the case is closed with No Action;
- 6. Reports of precedent-setting cases are to be maintained permanently. FSIS will offer such reports to the National Archives and Records Administration ten (10) years after the end of the fiscal year in which the case is closed; and
- 7. Investigative Sample Retention:
 - a. Investigative samples held at FSIS laboratories may be disposed of upon a determination that no action will be taken with regard to the sample;
 - b. Investigative samples held at FSIS laboratories that support cases pending disposition may be disposed of subsequent to issuance of a closing action (e.g., NOW or LOI); and
 - c. Investigative samples held at FSIS laboratories that support cases pending litigation may be disposed of after a final disposition in the case and all legal proceedings or appeals have been exhausted.

NOTE: When the retention schedule has been met for administrative, criminal, or civil case files or other investigative reports, the program area (e.g., OIEA/CID regional office) with responsibility for the disposal of all evidentiary material related to the case, is responsible for notifying the FSIS laboratory.

B. Evidence is to be disposed of in the following manner:

1. All evidence and all copies of evidence, including electronic records, are to be destroyed by shredding or incineration, except for personal property evidence for which a Property Receipt was issued;
2. Return personal property evidence for which a Property Receipt was issued to the property owner; and
3. Document the disposal of all evidence in Section III of the Evidence Receipt and Chain of Custody form, provide it to the supervisory official for verification of disposal, and update the ANet/ICS record with the actual evidence destruction date.

CHAPTER IV - RESPONSIBILITIES

I. PROGRAM EMPLOYEES

The program employee who collects evidence is to:

1. Ensure the proper application of methods and procedures for collection, safeguarding, and disposal of evidence in accordance with this directive during surveillance, investigative, or other activities to prevent evidence from loss, unauthorized alteration, mishandling, or other actions that may affect its integrity;
2. Initial and date the back of all evidentiary documents, records, or items for evidence authentication, except original property, as previously defined in this directive;
3. Establish and maintain identity of investigative samples from the time of collection until receipt at the laboratory in accordance with this directive;
4. Upon collection of all evidentiary items, prepare an Evidence Receipt and Chain of Custody form in the ANet/ICS to establish identification of the evidence, initiate the chain of custody, and provide for evidence authentication;
5. When personal property is collected as evidence, complete a Property Receipt and provide the owner or custodian of the property with a copy;
6. When an evidentiary item is such that the Evidence Receipt and Chain of Custody form cannot easily accompany or be attached to the item, maintain the Evidence Receipt and Chain of Custody form with the case evidence;
7. Make copies of documentary evidence to be used in the investigative report;
8. Document transfers of evidence in Section II of the Evidence Receipt and Chain of Custody form to maintain the chain of custody; and
9. Ensure that the methods and procedures set forth in this directive are followed during liaison activities with other Federal, State, and local law enforcement agencies in the collection, safeguarding, and disposal of evidence, as applicable.

II. EVIDENCE OFFICER

The Evidence Officer (EO) is responsible for maintaining control of, and accountability for, all evidentiary items for each assigned investigation. In OIEA/CID, the EO will usually be the lead CID Investigator (case agent) but may be another program employee as designated by the RD. In OFO, the EO will usually be the DCS but may be another program employee as designated by the DM. In OA/ICS, the EO is to be designated by the Director. The EO is to:

1. Protect all incoming evidentiary items from loss, unauthorized alteration, mishandling, or other actions that may affect their integrity;
2. Maintain all original evidence and chain of custody in a secure, controlled-access area;
3. Generate in the ANet/ICS, a hard-copy of the Evidence Log for each assigned investigation as necessary to audit the evidence for each investigation;
4. Arrange for and document in Section II of the Evidence Receipt and Chain of Custody form the receiving of each piece of evidence and subsequent transfer, release, or return of evidence for laboratory analysis, investigative use, use in court, or as otherwise necessary;
5. Serve as a liaison with other FSIS program areas or other Federal, State, or local law enforcement agencies for transfers, releases, and returns of evidence for laboratory analysis, investigative use, or use in court;
6. Conduct periodic inventory of evidence for each assigned investigation to monitor control of and ensure accountability for that evidence; and
7. Arrange for the proper disposal of evidence in accordance with the schedules for evidence retention in this directive.

III. PROGRAM OFFICIALS

The OIEA CID RD, OFO DM, OA ICS Director, and ELD Director, or designees, are to:

1. Establish security for evidence (e.g., evidence room, locked cabinet), including limited access to secure areas;
2. Assign an EO for each investigation in their area (e.g., region, district) of responsibility;
3. Receive and provide FSIS laboratory analysis results to the lead CID Investigator, EO, or other program employee;
4. Conduct periodic reviews of evidence, evidence logs, and evidence receipts to monitor control of and accountability for evidence; and
5. Ensure the timely and proper disposal of evidence in accordance with schedules and procedures in this directive, including notifying the appropriate laboratory when it is no longer necessary to hold investigative samples.

IV. LABORATORY PERSONNEL

The FSIS laboratory personnel are to:

1. Document receipt of investigative sample evidence in Section II of the Evidence Receipt and Chain of Custody form to maintain the chain of custody;

2. Document any subsequent transfer, release, or return of evidence for investigative use, use in court, or as otherwise necessary;
3. Follow OPHS laboratory internal guidelines in the analysis, storage, and disposal of investigative sample evidence;
4. Complete Section III of the Evidence Receipt and Chain of Custody form to document the final disposal action of investigative sample evidence; and
5. Return the completed Evidence Receipt and Chain of Custody form to the appropriate program area office.

V. QUESTIONS

Refer questions regarding this directive through supervisory channels.

A handwritten signature in black ink that reads "Robert J. Wagner". The signature is written in a cursive style with a large, stylized initial "R".

Assistant Administrator
Office of Policy and Program Development