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

FSIS DIRECTIVE

5500.2
Revision 7

11/8/18

SIGNIFICANT INCIDENT RESPONSE

I. PURPOSE

This directive outlines the procedures the FSIS Emergency Management Committee (EMC) and programs within FSIS are to follow while managing significant incidents. A significant incident is one that presents a grave, or potentially grave, threat to public health, to the safety of FSIS-regulated products, or FSIS personnel. FSIS is revising this directive to further clarify when a non-routine incident (e.g., natural disaster) becomes a significant incident and may require the creation of an incident report (IR). This directive also outlines the internal FSIS communication protocol for threats to the food and agriculture sector that may lead to a significant incident.

KEY POINTS:

- *Contains information on what developments trigger an IR*
- *Provides instructions for completing an IR*
- *Defines the EMC and its activities*
- *Provides information on sharing updates to IRs when the FSIS Incident Management System (FIMS) is unavailable*
- *Outlines internal FSIS protocol for communicating threat information*

II. CANCELLATION

FSIS Directive 5500.2, Revision 6, *Significant Incident Response*, 3/9/14

FSIS Directive 5420.2, Revision 1, *Homeland Security Threat Condition Response – Handling of FSIS Laboratory Samples Under Declared Heightened Threat Conditions*, 1/26/05

FSIS Directive 5420.5, *Revision 3, Homeland Security Threat Condition Response – Intelligence Reports and Communication*, 7/16/10

FSIS Directive 5420.6, Revision 1, *Homeland Security Threat Condition Response – Information Technology Monitoring Procedures*, 1/26/05

FSIS Directive 5420.7, *Revision 1, Homeland Security Threat Condition Response – Human Health Monitoring and Surveillance*, 1/26/05

FSIS Directive 5420.8, Revision 1, *Homeland Security Threat Condition Response – Communication and Public Affairs Procedures*, 1/26/05

III. BACKGROUND

A. A significant incident presents a grave, or potentially grave, threat to public health or to the safety of FSIS-regulated products. Examples of significant incidents include, but are not limited to, the following:

1. Life-threatening or widespread human illnesses potentially implicating FSIS-regulated product that lead to an FSIS foodborne illness investigation, as described in FSIS Directive 8080.3, *Food Borne Illness Investigations;*

2. Class I recalls resulting from one or more consumer illnesses, or injuries (injury can occur when foreign material contaminates the product. Factors include: size, material, and intended customer (i.e. toddler food)) involving FSIS-regulated products;

3. Intentional contamination of FSIS-regulated products;

4. Threat information received from the intelligence community that is determined by the Office of the Administrator (OA) Chief Operating Officer (COO) to pose a significant threat or risk to FSIS personnel or the food and agriculture sector (e.g., a National Terrorism Advisory System alert or bulletin issued by the Department of Homeland Security);

5. A foreign animal disease as described in FSIS Directive 6000.1, *Responsibilities Related to Foreign Animal Diseases and Reportable Conditions*, is detected in animals presented for slaughter within the United States (U.S.);

6. Detection of an animal disease with potentially significant public health implications for FSIS-regulated products by FSIS Public Health Veterinarians or other government source;

7. Illegally imported or smuggled product in the U.S. where there is a reasonable probability that the consumption of the product will pose a serious health hazard;

8. High-risk FSIS-regulated imported product in the U.S.;

9. Suspicious activities observed by, or made known to FSIS personnel (e.g., bomb threats); and

10. Non-routine incidents (e.g., Food and Drug Administration enforcement actions, or law enforcement) to protect public health (e.g., stolen trucks, findings of excessive levels of chemical residues, preparation for and support of a Special Event/National Special Security Event) involving the adulteration, or potential adulteration, of FSIS-regulated product, which requires significant coordination, sharing, or expenditure of resources among program areas and other regulatory agencies.

B. Additional situations that FSIS may consider to be significant incidents include:

1. Natural disasters (e.g., wildfires, hurricanes, floods, tornadoes, and earthquakes) that impact FSIS employees, regulated facilities, or regulated products;

2. Terrorist attacks on the nation's critical food and agriculture sector infrastructure; and

3. Other incidents requiring a national coordinated response that result in the activation of the Emergency Support Function #11 (ESF#11) at the Federal Emergency Management Agency, National Response Coordination Center (NRCC), which is described in the Agriculture and Natural Resources Annex to the National Response Framework.

IV. NOTIFICATION OF THREAT FROM INTELLIGENCE COMMUNITY

A. All FSIS personnel need to know the protocol for communicating threat information that may be related to the food and agriculture sector. Threat information from the intelligence community is to be communicated through the following:

1. The FSIS COO or designee is the primary point of contact for receipt of threat information from the intelligence community (e.g., Department of Homeland Security);

2. If a threat has the potential or is expected to affect food or agriculture, the COO or designee is to inform the FSIS Management Council (MC) (i.e., the FSIS Administrator, Deputy Administrator, Assistant Administrators (AAs), Deputy AAs, and other members of the Senior Executive Service and Agency senior managers as designated by the Administrator);

3. The COO or designee will determine the appropriate distribution of the threat information in coordination with FSIS' Office of Field Operations (OFO), Office of Investigation, Enforcement and Audit (OIEA), Office of Public Affairs and Consumer Education (OPACE), and Office of Public Health Science (OPHS), and ensure employees, stakeholders, and the public are notified, as appropriate; and

4. In the event of a significant incident, the FSIS EMC may be alerted or activated and other response actions taken pursuant to this directive.

B. Frontline supervisors are to ensure that any notifications distributed pursuant to this directive are available to inspection program personnel (IPP) in the establishment.

C. As soon as frontline supervisors are notified of threat information, they are to inform establishment management of the alert. Frontline supervisors are to document their discussion with establishment management in a memorandum of interview (MOI) (see FSIS Directive 5010.1, *Food Safety Related Topics for Discussion During Weekly Meetings with Establishment Management*).

D. The COO is to notify the MC of any changes in threat information, including when the period of concern has expired. The COO is to coordinate with OFO, OIEA, OPACE, and OPHS to notify employees, stakeholders, and the public as appropriate. Field supervisors are to advise IPP in the establishment and establishment management of the change in threat status.

E. If FSIS personnel observe a potentially significant incident, they are to report it through supervisory channels**.**

V. FSIS PERSONNEL RESPONSIBILITIES FOR REPORTING A SIGNIFICANT INCIDENT

A. FSIS personnel are to immediately report any potentially significant incident as defined in Section III through supervisory channels. The information reported, at a minimum, is to include:

1. The name of the person who reported the incident;

2. The date and time of the incident;

3. The location of the incident;

4. The type of threat, hazard, or disease;

5. The type of product involved, and

6. The number of reported illnesses, injuries, and deaths (if applicable).

B. Designated FSIS personnel (see attachment) with access to FIMS are to review the incident information and, if appropriate, develop an IR and submit the report into FIMS for the approving official to review.

C. For Class I recalls involving one or more illnesses or one or more injuries (see Section III.A. 2.), the EMC representative of OPACE is to initiate an IR in FIMS and post the recall release.

D. For significant incidents where the NRCC has activated ESF#11 in response to a natural disaster, Significant Incident Preparedness and Response Staff (SIPRS) will initiate an IR if one has not yet been entered by another program area.

E. For all significant incidents that involve law enforcement agencies or the notification of the Office of Inspector General, the OIEA, Compliance and Investigation Division (CID) is to be notified by phone and a follow up e-mail by the reporting program area.

F. When the OPHS Applied Epidemiology Staff (AES) initiates a FSIS foodborne illness investigation per FSIS Directive 8080.3, and determines that an IR is needed because it is a significant incident (see Section III), the AES lead investigator is to enter information about the investigation into the FIMS.

G. As needed, the Food Emergency Response Network (FERN) laboratories may be used to respond to food-related emergencies.

H. The COO may receive notification of a significant incident from the National Biosurveillance Integration Center (NBIC) or one of its member agencies. Once the information is received, the COO or designee is to discuss the information with the relevant program areas to determine whether an IR or an alert notification through FIMS to the EMC and MC is warranted. Additional details about alerts are provided in Section VIII.

VI. COMPLETING AN INCIDENT REPORT

A. The “FIMS User Manual” in FIMS contains detailed information on how to complete an IR.

B. The electronic IRs can be created and accessed on an FSIS-issued computer through FIMS via the following intranet link: https://FIMS.fsis.usda.gov.

C. The electronic IR in FIMS automatically saves the IR by its case number. The case number is derived using the following format: year, month, day, number of IRs entered that day (e.g., 20170130-1 means this is the first IR reported on January 30, 2017).

D. All approved IRs in FIMS are automatically forwarded to all AAs or their designees, the EMC representatives who are on duty, and to the SIPRS for review following the process outlined in the attachment, if they set up their notification preferences. If they did not set up these preferences, notifications need to be accessed in FIMS under Notifications and Subscriptions.

E. Designated staff from involved program areas are to update the IR through FIMS as often as necessary, but at least once per week or as directed in specific agency guidance. The most recent information will appear first on the IR. Whenever certain fields in the IR are updated, an e-mail notification will be sent to FIMS users described in Section D above, and users who have subscribed to the IR.

VII. FIMS OR E-MAIL SYSTEM OUTAGE

A. If the FIMS system is non-operational, the person who generates or updates the IR is to send the information about the incident to their AA or designee and the COO or designee as an attachment to an e-mail or via fax. The COO fax information is on the EMC roster, which can be requested from the EMC duty officer. Information can also be e-mailed to ERI-Mail@fsis.usda.gov.

B. Upon receipt of the information, SIPRS is to manually, through a Word document or by attaching the faxed information, update an IR using the approved FSIS form (e.g., 5500-4, 5500-8). This information is to be shared with the EMC representative of each program area. The EMC program area representative is to share this information with his or her program area's FIMS user community by e-mail or fax until FIMS is restored.

C. In the event that fax or e-mail systems are not available or operational, the person who generates the IR is to notify the EMC Senior Executive Duty Officer (SEDO) so the IR can be updated. The person is also to inform their AA or designee or their program EMC representative, and the SIPRS EMC representative. Their AA or designee is to share the information immediately with the COO or designee and decide whether further action is warranted.

D. When e-mail and fax become available, the person who generates the IR is to notify the same personnel described in Section C above and follow the FIMS outage procedures described in Sections A and B above. For information received during the e-mail and fax outage, the person who generated the IR should discuss with their AA or designee or their program EMC representative, and the SIPRS EMC representative if it still needs to be shared with others on the EMC for situational awareness.

E. When the FIMS system becomes operational, the person who initiated or updated the IR during the outage is to enter all the information from the outage period about the incident into FIMS.

VIII. REVIEWING THE IR, ALERTING AND ACTIVATING THE EMC

A. The COO or designee and the AA responsible for the IR (from the program where the IR originated), or their designees, are to review the approved IR and, as appropriate, determine:

1. That no additional alert or activation is required;

2. That the EMC is to be alerted; or

3. That the EMC is to be activated.

B. The COO or designee and the AA responsible for the IR (or designees) are also to determine, as appropriate, what further actions need to be taken on the IR.

C. If, after the COO or designee and representatives of the program areas relevant to the IR discuss the status of the significant incident and determine that the incident is resolved, and no further actions or monitoring are required, a representative of the program that originated the IR is to recommend closure in the comment section of FIMS. Once this recommendation is in FIMS, the EMC Duty Officer will request recommendations for closure from all programs involved in the incident. Once recommendations for closure are added to the FIMS comment section by each of the programs involved in the incident, the EMC Duty Officer is to close the IR.

NOTE: Closed IRs can still be updated with new information if necessary.

D. An IR can be classified as "restricted" when it contains sensitive information that is not to be shared with all FIMS users. The COO or designee will work with the program area with primary responsibility for the IR to determine whether access to the IR should be restricted. They are to consult with other program area representatives as needed to make the final determination. Together, they will determine who will have access to the restricted IR.

E. If the COO or designee and the AA responsible for the IR (or designee) determine that an incident may warrant further discussion by the EMC, SIPRS is to send a notification alert through FIMS to the EMC representatives. This notification alerts the EMC representatives that there is a significant incident that may warrant an EMC alert or activation.

F. If the COO or designee and the AA responsible for the IR (or designee) determine that the EMC needs to be activated (e.g., to decide a plan of action), SIPRS is to send an activation notification through FIMS to the EMC representatives on duty for each program area. The message is to provide instructions on where to convene or how to participate in a conference call.

G. The EMC Duty Officer is to forward a copy of the notification for alerts and activations to the MC, the Office of the Under Secretary for Food Safety, the OA, and the USDA Office of Homeland Security (OHS).

IX. EMC

A. The EMC is comprised of senior management (AA or designee) from each of the FSIS program areas. Each program area EMC representative is to have the authority to commit, as necessary, the resources of his or her respective program area in responding to the incident. The EMC duty roster is available in FIMS and is issued by e-mail weekly to all employees who serve on the EMC, as well as the Office of the Under Secretary for Food Safety, the OA, and the OHS. The list contains on-call members with their contact information for each program area.

B. The EMC may be alerted or activated at any time, on any day of the year, to address and manage the Agency's response to a significant incident as defined in Section III of this directive. As described in FSIS Directive 8080.1, *Recall of Meat and Poultry Products,* the EMC can also be activated if the Recall Committee or the AAs are unable to reach consensus on whether the Agency should request that a company conduct a recall, or when there may be need for a public health alert related to a foodborne illness investigation.

C. The SEDO serves as the initial Incident Commander (IC). The IC coordinates the work of the EMC in response to a specific significant incident. Depending on the nature, scope, and complexity of the incident, the initial or current IC may designate any program area representative as IC to coordinate key activities critical to the management of the incident. The IC is to ensure that Agency subject matter experts are included in EMC meetings.

D. The Duty Officer and SEDO for the EMC maintain an up-to-date roster of on-call EMC members, including home, work, and cell phone numbers and e-mail addresses. The Duty Officer, in conjunction with the SEDO, also manage IRs, monitors FIMS readiness, and prepares situation and spot reports for the USDA's Operations Center as information becomes available, or as requested by the Department.

E. SIPRS maintains the FSIS Continuity of Operations Plan, in conjunction with the OHS.

X. THE WORK OF THE EMC

A. Upon alert or activation, the EMC evaluates the information provided in the IR and determines what information is needed to complete the assessment of the significant incident. The EMC also develops and implements an incident action plan (if needed), which is posted to the IR in FIMS. The execution of

the incident action plan is monitored by the IC through FIMS.

B. The EMC coordinates the development of responses to questions about the incident, including responses to questions about illness prevention, hazard detection, incident containment, and remediation. The EMC also recommends Agency actions to detect, respond to, and mitigate the hazard that caused the incident, including the formation of an Incident Investigation Team (see FSIS Directive 5500.3, *Incident Investigations Team Reviews*).

C. The IC provides progress reports to the MC, as requested. All program areas involved in the incident are to routinely provide updates using the IR in FIMS to assist the IC in tracking the incident response, reporting progress, and maintaining relevant documents and a chronology of events.

D. When the incident has been resolved, the IC, in conjunction with the EMC members, is to deactivate the EMC and advise the Office of the Under Secretary for Food Safety, the OA, the MC, and the OHS. The EMC Duty Officer will notify all EMC representatives and other parties through FIMS, and the IR will be closed simultaneously with the deactivation.

XI. COMPLETING FSIS FORM 5500-8, IMPACT OF SIGNIFICANT INCIDENTS ON ESTABLISHMENTS (INCLUDING IMPORT ESTABLISHMENTS) AND WAREHOUSES, AND THE AUTOMATED EMPLOYEE TRACKING SHEET

A. EMC representatives are to coordinate the collection and submission of information necessary to complete an FSIS Form 5500-8 or the Automated Employee Tracking Sheet in FIMS. These forms track the operational status of official establishments (including import establishments), in-commerce facilities that handle FSIS-regulated product (e.g., distributors, warehouses), FSIS offices, laboratories, and FSIS employees affected by a significant incident, such as an earthquake, flooding, fire, or hurricane. All FSIS program areas are to submit a program specific 5500-8 using FIMS for establishments/firms that have their operational status affected by a significant incident. The Automated Employee Tracking Sheet is used to supply information on employee status during a significant incident.

NOTE: Authorized users can access the forms through FIMS at https://FIMS.fsis.usda.gov. For those individuals without access to FIMS, Form 5500-8 is available on Inside FSIS at https://inside.fsis.usda.gov.

B. SIPRS is to notify the appropriate EMC representatives from the relevant areas to collect information about the status of their employees and operational status of establishments or facilities in the affected areas by contacting their local program area offices. When contacting the District or Regional Offices via e-mail, SIPRS will ensure they send a copy to the program area EMC representative.

C. The EMC representative is then to notify the appropriate personnel within his or her program, for example, the District Manager or CID Regional Director, to collect the information and complete FSIS Form 5500-8, and if necessary the Automated Employee Tracking Sheet, in FIMS. FSIS field personnel may need to supply information on employee status, and whether official establishments or firms are operational as a result of the significant incident.

D. To complete FSIS Form 5500-8 in FIMS, FSIS personnel may need to contact other FSIS personnel, such as Front-line Supervisors; Consumer Safety Officers; Enforcement, Investigations, and Analysis Officers; Investigators; or Headquarters personnel. The following information is needed to complete FSIS Form 5500-8:

1. The specific IR # that relates to the incident requiring a FSIS Form 5500-8 to be filled out if this is done manually. If it is done in FIMS, the IR number will prepopulate;

2. For OFO and OIEA, the official establishment numbers for establishments or firms that are not operating:

a. For OFO, the establishment names, location (city, state), establishment size, establishment type (Federal/Talmadge-Aiken), and slaughter and processing volumes are prepopulated;

b. For OIEA, the addresses are prepopulated. The contact information, and number of buildings impacted at high-volume distribution points (e.g., wholesale grocery suppliers or transportation centers) that are not operating need to be entered into the FSIS Form 5500-8. In addition, poundage of product(s) impacted, detained, or seized also needs to be entered;

3. For both OFO and OIEA, the reason why the establishment or firm is not operational:

    a. Insufficient facility personnel present;

    b. Damage from flooding;

    c. Building destroyed;

    d. No electricity;

    e. Hazardous weather; or

    f. Other (specify); and

4. For all program areas reporting on damage to or closure of FSIS-occupied office space, the person reporting needs to have the name of the building, address, and reason for its non-operation.

F. FSIS program areas are to enter the following information to complete the Automated Employee Tracking Form if necessary:

1. Number of employees that normally work in their program area, broken down by state (location of duty station);

2. Number of employees from their program area that are displaced from their residence and/or duty station, broken down by state;

3. Number of employees from their program area that are absent for any reason, broken down by state:

    a. Number of employees from their program area that are not accounted for, broken down by state; and

    b. The number of employees from their program area that are deceased, injured or ill.

G. After the initial submission of a completed FSIS Form 5500-8 and/or the Automated Employee Tracking Sheet, the forms will be automatically attached to the IR. Program areas are to edit the forms attached to the IR in FIMS each time there is a change to any of their entries', or if additional entries need to be made. After saving the changes to FSIS Form 5500-8 or to the Automated Employee Tracking Sheet in FIMS, SIPRS will be notified by FIMS that the information is available for review. Daily updates are not needed if there is no change in status unless otherwise requested.

XII. OIEA RESPONSIBILITIES

A. OIEA personnel are to develop an Investigative Response Plan and attach the plan to the IR within 12 hours, or when the IR is approved for food safety or food defense events including natural disasters, intentional contamination, or significant economic adulteration.

1. OIEA personnel are to input an Investigative Plan (see FSIS Directive 8010.2, *Investigative Methodology*) for all IR approved illness outbreak investigations; and

2. OIEA personnel are to input a response plan for all IR approved natural disasters or threats of natural disasters. Response plan templates can be found on the Library page in FIMS.

B. OIEA personnel are to ensure that within 12 hours after the IR is approved in FIMS, a timeline is developed and submitted for Investigative and Response Plans (see FSIS Directive 8010.2). OIEA personnel are to update the timelines daily. Timeline templates can be found on the Library page in FIMS.

XIII. QUESTIONS

Refer questions to SIPRS through e-mail at ERI-Mail@fsis.usda.gov or by telephone at 202-981-6889.

Assistant Administrator
Office of Policy and Program Development

Attachment

Incident Report (IR) Process Via FSIS' Incident Management System (FIMS) Based on Incident Information

Program Area	**Incident Information Sources**	**FSIS Personnel with Access to the FIMS for IR Development**	**FSIS Personnel Responsible for IR Review**	**FSIS Personnel Responsible for Approving IR**
OA – Office of the Administrator	External Federal Agencies	OA- Chief of Staff/Chief Information Officer (CIO)/Chief Financial Officer (CFO)/Office of International Coordination (OIC COO/Designee/Duty Officer (DO)	OA- Chief of Staff/ CIO/CFO/OIC/ Designee COO/Designee	OA- Chief of Staff/ CIO/CFO/OIC/ Designee COO/Designee
COO – The Chief Operating Officer	OA External Agencies Other Program Offices	COO/Designee/DO (COO also has access to every program's IR for further development)	COO/Designee	COO/Designee
OIEA – Office of Investigation, Enforcement and Audit	External Agencies CID Industry	CID-Director, Deputy Director, Compliance Specialist, Regional Director, Supervisory Compliance Investigator, Sr. Compliance Investigator, Compliance Investigator COO/Designee/DO	Regional Director	Regional Director* *cc: CID Director
	Management Control and Audit Division (MCAD) External - State MPI Programs	Director MCAD COO/Designee/DO	Director MCAD	Director MCAD

Program Area	Incident Information Sources	FSIS Personnel with Access to the FIMS for IR Development	FSIS Personnel Responsible for IR Review	FSIS Personnel Responsible for Approving IR
OPACE – Office of Public Affairs and Consumer Education	USDA Meat and Poultry Hot Line Information	USDA Meat and Poultry Hot Line Specialist and Manager COO/Designee/DO	FSES Director	OPACE AA/ Designee
	External Sources	Director: Executive Correspondence and Issues Management Staff (ECIMS), Congressional and Public Affairs Staff (CPAS), Food Safety Education Staff (FSES), Freedom of Information Act Staff (FOIAS), Web and Digital Communications Staff (WDCS) COO/Designee/DO	Director: ECIMS, CPAS, FSES, FOIAS, WDCS	OPACE AA/ Designee
OFO – Office of Field Operations	External Agencies Inspectors-in-charge (IICs) Import Inspection Personnel Industry	District Manager (DM) or Deputy District Manager (DM)/Designee, Case Specialist, Director Resource Management and Financial Planning Staff or Designee, Front Line Supervisors, Recall Management and Technical Analysis Division COO/Designee/DO	OFO AA/Designee, DM, DDM, or Designee	DM, DDM/Designee

Program Area	Incident Information Sources	FSIS Personnel with Access to the FIMS for IR Development	FSIS Personnel Responsible for IR Review	FSIS Personnel Responsible for Approving IR
OPPD – Office of Policy and Program Development	External Agencies Industry	Director: Policy Development Staff, Policy Analysis Staff, Labeling and Program Delivery Staff, Risk Management and Innovation Staff COO/Designee/DO	OPPD AA/ Designee	OPPD AA/ Designee
OPHS – Office of Public Health Science	External Agencies, State and Local Partners, Consumer Complaint Monitoring System (CCMS) Staff, Applied Epidemiology Staff (AES) investigative staff	AES Director/Designee, CCMS Staff, AES investigative Staff COO/Designee/DO	OPHS AA/Designee AES Director or Designee	OPHS AA/Designee AES Director or Designee
	Laboratories, CDC Liaison	OPHS AA Lab Directors COO/Designee/DO	OPHS AA/Designee	OPHS AA/Designee
OEED – Office of Employee Experience and Development	Regional Trainers and other FSIS personnel	OEED AA Training Transformation and Distance Learning, and Employee Engagement and Recognition Staffs COO/Designee/DO	OEED AA/Designee	OEED AA/Designee

Program Area	Incident Information Sources	FSIS Personnel with Access to the FIMS for IR Development	FSIS Personnel Responsible for IR Review	FSIS Personnel Responsible for Approving IR
OM – Office of Management	Administrative Services Division (ASD), Safety and Physical Security Branch (SPSB)	OM AA/ASD Director/SPSB Director/SPS Specialists/or Designee COO/Designee/DO	OM AA/Designee	OM AA/Designee