December 17, 2003

Guidance for Industry

Retail Food Stores and Food Service Establishments: Food Security Preventive Measures Guidance

FINAL GUIDANCE

Additional copies are available from:
Office of Compliance
Center for Food Safety and Applied Nutrition
Food and Drug Administration
5100 Paint Branch Parkway
College Park, MD 20740
(Tel) 301-436-2359
http://www.cfsan.fda.gov/guidance.html

Purpose and Scope:

This guidance is designed as an aid to operators of retail food stores and food service establishments (for example, bakeries, bars, bed-and-breakfast operations, cafeterias, camps, child and adult day care providers, church kitchens, commissaries, community fund raisers, convenience stores, fairs, food banks, grocery stores, interstate conveyances, meal services for home-bound persons, mobile food carts, restaurants, and vending machine operators). This is a very diverse set of establishments, which includes both very large and very small entities.

This guidance identifies the kinds of preventive measures they may take to minimize the risk that food under their control will be subject to tampering or other malicious, criminal, or terrorist actions. Operators of food retail food stores and food service establishments are encouraged to review their current procedures and controls in light of the potential for tampering or other malicious, criminal, or terrorist actions and make appropriate improvements.

This guidance is designed to focus operators' attention sequentially on each segment of the food delivery system that is within their control, to minimize the risk of tampering or other malicious, criminal, or terrorist action at each segment. To be successful, implementing enhanced preventive measures requires the commitment of management and staff. Accordingly, FDA recommends that both management and staff participate in the development and review of such measures.

FDA's guidance documents, including this guidance, do not establish legally enforceable responsibilities. Instead, guidances describe the Agency's current thinking on a topic and should be viewed only as recommendations, unless specific regulatory or statutory requirements are cited. The use of the word *should* in Agency guidances means that something is suggested or recommended, but not required.

Limitations:

Not all of the guidance contained in this document may be appropriate or practical for every retail food store or food service establishment, particularly smaller facilities. FDA recommends that operators review the guidance in each section that relates to a component of their operation, and assess which preventive measures are suitable. Example approaches are provided for many of the preventive measures listed in this document. These examples should not be regarded as minimum standards. Nor should the examples provided be considered an inclusive list of all potential approaches to achieving the goal of the preventive measure. FDA recommends that operators consider the goal of the preventive measure, assess whether the goal is relevant to their operation, and, if it is, design an approach that is both efficient and effective to accomplish the goal under their conditions of operation.

Structure:

This guidance is divided into five sections that relate to individual components of a retail food store or food service establishment operation: management, human element-staff, human element-public, facility, and operations.

Related Guidance:

FDA has published two companion guidance documents on food security, entitled, "Food Producers, Processors, and Transporters: Food Security Preventive Measures Guidance" and "Importers and Filers: Food Security Preventive Measures Guidance" to cover the farm-to-table spectrum of food production. Both documents are available at: http://www.cfsan.fda.gov/~dms/guidance.html.

Additional Resources:(*)

A process called Operational Risk Management (ORM) may help prioritize the preventive measures that are most likely to have the greatest impact on reducing the risk of tampering or other malicious, criminal, or terrorist actions against food. Information on ORM is available in the Federal Aviation Administration (FAA) System Safety Handbook, U.S. Department of Transportation, FAA, December 30, 2000, Chapter 15, Operational Risk Management. The handbook is available at: http://www.asy.faa.gov/Risk/SSHandbook/Chap15_1200.PDF (January 2006 updated link: http://www.faa.gov/library/manuals/aviation/risk_management/ss_handbook/media/Chap15_1200.PDF).

The U.S. Department of Transportation, Research and Special Programs Administration has published an advisory notice of voluntary measures to enhance the security of hazardous materials shipments. It is available at: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2002_register&docid=02-3636-filed.pdf. The notice provides guidance to shippers and carriers on personnel, facility and en route security issues.

The U.S. Postal Service has prepared guidance for identifying and handling suspicious mail. It is available at: http://www.usps.com/news/2001/press/mailsecurity/postcard.htm.

The Federal Anti-Tampering Act (18 USC 1365) makes it a federal crime to tamper with or taint a consumer product; to attempt, threaten, or conspire to tamper with or taint a consumer product; or make a false statement about having tampered with or tainted a consumer product. Conviction can lead to penalties of up to $100,000 in fines and up to life imprisonment. The Act is available at: http://www.fda.gov/opacom/laws/fedatact.htm.

The National Infrastructure Protection Center (NIPC) serves as the federal government's focal point for threat assessment, warning, investigation, and response for threats or attacks against U.S. critical infrastructure. The NIPC has identified the food system as one of the eight critical infrastructures, and has established a public-private partnership with the food industry, called the Food Industry Information Sharing and Analysis Center (Food Industry ISAC). The NIPC provides the Food Industry ISAC with access, information, and analysis, enabling the food industry to report, identify, and reduce its vulnerabilities to malicious attacks, and to recover from such attacks as quickly as possible. In particular, the NIPC identifies credible threats and crafts specific warning messages to the food industry. Further information is available at http://www.nipc.gov/ and http://www.foodisac.org/.

Finally, FDA encourages trade associations to evaluate the preventive measures contained in this guidance document and adapt them to their specific products and operations and to supplement this guidance with additional preventive measures when appropriate. FDA welcomes dialogue on the content of sector specific guidance with appropriate trade associations.

Retail Food Store and Food Service Establishment Operations:

Management

FDA recommends that retail food store and food service establishment operators consider:

- Preparing for the possibility of tampering or other malicious, criminal, or terrorist events
    - assigning responsibility for security to knowledgeable individual(s)
    - conducting an initial assessment of food security procedures and operations, which we recommend be kept confidential
    - having a crisis management strategy to prepare for and respond to tampering and other malicious, criminal, or terrorist actions, both threats and actual events, including identifying, segregating, and securing affected products
    - planning for emergency evacuation, including preventing security breaches during evacuation
    - becoming familiar with the emergency response system in the community
    - making management aware of 24-hour contact information for local, state, and federal police/fire/rescue/health/homeland security agencies
    - making staff aware of who in management they should alert about potential security problems (24-hour contacts)
    - promoting food security awareness to encourage all staff to be alert to any signs of tampering or malicious, criminal, or terrorist actions or areas that may be vulnerable to such actions, and to report any findings to identified management (for example, providing training, instituting a system of rewards, building security into job performance standards)
    - having an internal communication system to inform and update staff about relevant security issues
    - having a strategy for communicating with the public (for example, identifying a media spokesperson, preparing generic press statements and background information, and coordinating press statements with appropriate authorities)
- Supervision
    - providing an appropriate level of supervision to all staff, including cleaning and maintenance staff, contract workers, data entry and computer support staff, and especially, new staff (for example, supervisor on duty, periodic unannounced visits by supervisor, daily visits by supervisor, two staff on duty at same time, monitored video cameras, off-line review of video tapes, one-way and two-way windows, customer feedback to supervisor of unusual or suspicious behavior by staff)
    - conducting routine security checks of the premises, including utilities and critical computer data systems (at a frequency appropriate to the operation) for signs of tampering or malicious, criminal, or terrorist actions, or areas that may be vulnerable to such actions
- Investigation of suspicious activity
    - investigating threats or information about signs of tampering or other malicious, criminal, or terrorist actions
    - alerting appropriate law enforcement and public health authorities about any threats of or suspected tampering or other malicious, criminal, or terrorist actions
- Evaluation program
    - evaluating the lessons learned from past tampering or other malicious, criminal, or terrorist actions and threats
    - reviewing and verifying, at least annually, the effectiveness of the security management program (for example, using knowledgeable in-house or third-party staff to conduct tampering or other malicious, criminal, or terrorist action exercises and to challenge computer security systems), revising accordingly (using third-party or in-house security expert, where possible), revising the program accordingly, and keeping this information confidential
    - performing random food security inspections of all appropriate areas of the facility (including receiving and storage areas, where applicable) using knowledgeable in-house or third-party staff, and keeping this information confidential
    - verifying that security contractors are doing an appropriate job, when applicable

Human element -- staff

Under Federal law, retail food store and food service establishment operators are required to verify the employment eligibility of all new hires, in accordance with the requirements of the Immigration and Nationality Act, by completing the INS Employment Eligibility Verification Form (INS Form I-9). Completion of Form I-9 for new hires is required by 8 USC 1324a and nondiscrimination provisions governing the verification process are set forth at 1324b.

FDA recommends that retail food store and food service establishment operators consider:

- Screening (pre-hiring, at hiring, post-hiring)
    - examining the background of all staff (including seasonal, temporary, contract, and volunteer staff, whether hired directly or through a recruitment firm) as appropriate to their position, considering candidates' access to sensitive areas of the facility and the degree to which they will be supervised and other relevant factors (for example, obtaining and verifying work references, addresses, and phone numbers, participating in one of the pilot programs managed by the Immigration and Naturalization Service and the Social Security Administration [These programs provide electronic confirmation of employment eligibility for newly hired employees. For more information call the INS SAVE Program toll free at 1-888-464-4218, fax a request for information to (202) 514-9981, or write to US/INS, SAVE Program, 425 I Street, NW, ULLICO-4th Floor, Washington, DC 20536. These pilot programs may not be available in all states], having a criminal background check performed by local law enforcement or by a contract service provider [Remember to first consult any state or local laws that may apply to the performance of such checks])
- Note: screening procedures should be applied equally to all staff, regardless of race, national origin, religion, and citizenship or immigration status.
- Daily work assignments
    - knowing who is and who should be on premises, and where they should be located, for each shift
    - keeping information updated
- Identification
    - establishing a system of positive identification and recognition (for example, issuing uniforms, name tags, or photo identification badges with individual control numbers, color coded by area of authorized access), when appropriate
    - collecting the uniforms, name tag, or identification badge when a staff member is no longer associated with the establishment
- Restricted access
    - identifying staff that require unlimited access to all areas of the facility
    - reassessing levels of access for all staff periodically
    - limiting staff access to non-public areas so staff enter only those areas necessary for their job functions and only during appropriate work hours (for example, using key cards or keyed or cipher locks for entry to sensitive areas, color coded uniforms [remember to consult any relevant federal, state, or local fire or occupational safety codes before making any changes])
    - changing combinations, rekeying locks, and/or collecting the retired key card when a staff member who is in possession of these is no longer associated with the establishment, and additionally as needed to maintain security
- Personal items
    - restricting the type of personal items allowed in non-public areas of the establishment
    - allowing in the non-public areas of the establishment only those personal use medicines that are necessary for the health of staff (other than those being stored or displayed for retail sale) and ensuring that these personal use medicines are properly labeled and stored away from stored food and food preparation areas
    - preventing staff from bringing personal items (for example, lunch containers, purses) into nonpublic food preparation or storage areas
    - providing for regular inspection of contents of staff lockers (for example, providing metal mesh lockers, company issued locks), bags, packages, and vehicles when on company property (Remember to first consult any federal, state, or local laws that may relate to such inspections)
- Training in food security procedures
    - incorporating food security awareness, including information on how to prevent, detect, and respond to tampering or other malicious, criminal, or terrorist actions or threats, into training programs for staff, including seasonal, temporary, contract, and volunteer staff
    - providing periodic reminders of the importance of security procedures (for example, scheduling

meetings, providing brochures, payroll stuffers)
- encouraging staff support (for example, involving staff in food security planning and the food security awareness program, demonstrating the importance of security procedures to the staff)
- encouraging staff support (for example, involving staff in food security planning and the food security awareness program, demonstrating the importance of security procedures to the staff)

- Unusual behavior

  - watching for unusual or suspicious behavior by staff (for example, staff who, without an identifiable purpose, stay unusually late after the end of their shift, arrive unusually early, access files/information/areas of the facility outside of the areas of their responsibility; remove documents from the facility; ask questions on sensitive subjects; bring cameras to work)

- Staff health

  - being alert for atypical staff health conditions that staff may voluntarily report and absences that could be an early indicator of tampering or other malicious, criminal, or terrorist actions (for example, an unusual number of staff who work in the same part of the facility reporting similar symptoms within a short time frame), and reporting such conditions to local health authorities

Human element -- public

FDA recommends that retail food store and food service establishment operators consider:

- Customers

  - preventing access to food preparation and storage and dishwashing areas in the non-public areas of the establishment, including loading docks
  - monitoring public areas, including entrances to public restrooms (for example, using security guards, monitored video cameras, one-way and two-way windows, placement of employee workstations for optimum visibility) for unusual or suspicious activity (for example, a customer returning a product to the shelf that he/she brought into the store, spending an unusual amount of time in one area of the store)
  - monitoring the serving or display of foods in self-service areas (for example, salad bars, condiments, open bulk containers, produce display areas, doughnut/bagel cases)

- Other visitors (for example, contractors, sales representatives, delivery drivers, couriers, pest control representatives, third-party auditors, regulators, reporters, tours)

  - restricting entry to the non-public areas of the establishment (for example, checking visitors in and out before entering the non-public areas, requiring proof of identity, issuing visitors badges that are collected upon departure, accompanying visitors)
  - ensuring that there is a valid reason for all visits to the non-public areas of the establishment before providing access to the facility - beware of unsolicited visitors
  - verifying the identity of unknown visitors to the non-public areas of the establishment
  - inspecting incoming and outgoing packages and briefcases in the non-public areas of the establishment for suspicious, inappropriate or unusual items, to the extent practical

Facility

FDA recommends that retail food store and food service establishment operators consider:

- Physical security

  - protecting non-public perimeter access with fencing or other deterrent, when appropriate
  - securing doors (including freight loading doors, when not in use and not being monitored, and emergency exits), windows, roof openings/hatches, vent openings, ventilation systems, utility rooms, ice manufacturing and storage rooms, loft areas and trailer bodies, and bulk storage tanks for liquids, solids and compressed gases to the extent possible (for example, using locks, "jimmy plates," seals, alarms, intrusion detection sensors, guards, monitored video surveillance [remember to consult any relevant federal, state, or local fire or occupational safety codes before making any changes])
  - using metal or metal-clad exterior doors to the extent possible when the facility is not in operation, except where visibility from public thoroughfares is an intended deterrent (remember to consult any relevant federal, state, or local fire or occupational safety codes before making any changes)
  - minimizing the number of entrances to non-public areas (remember to consult any relevant federal, state, or local fire or occupational safety codes before making any changes)
  - accounting for all keys to establishment (for example, assigning responsibility for issuing, tracking, and retrieving keys)
  - monitoring the security of the premises using appropriate methods (for example, using security patrols [uniformed and/or plain-clothed], monitored video surveillance)
  - minimizing, to the extent practical, places in public areas that an intruder could remain unseen after work hours
  - minimizing, to the extent practical, places in non-public areas that can be used to temporarily hide intentional contaminants (for example, minimizing nooks and crannies, false ceilings)
  - providing adequate interior and exterior lighting, including emergency lighting, where appropriate, to facilitate detection of suspicious or unusual activity
  - implementing a system of controlling vehicles authorized to park in the non-public parking areas (for example, using placards, decals, key cards, keyed or cipher locks, issuing passes for specific areas and times to visitors' vehicles)
  - keeping customer, employee, and visitor parking areas separated from entrances to non-public areas, where practical

- Storage and use of poisonous and toxic chemicals (for example, cleaning and sanitizing agents, pesticides) in non-public areas

  - limiting poisonous and toxic chemicals in the establishment to those that are required for the operation and maintenance of the facility and those that are being stored or displayed for retail sale
  - storing poisonous and toxic chemicals as far away from food handling and food storage areas as practical
  - limiting access to and securing storage areas for poisonous or toxic chemicals that are not being held for retail sale (for example, using keyed or cipher locks, key cards, seals, alarms, intrusion detection sensors, guards, monitored video surveillance [remember to consult any relevant federal, state, or local fire codes before making any changes])
  - ensuring that poisonous and toxic chemicals are properly labeled
  - using pesticides in accordance with the Federal Insecticide, Fungicide, and Rodenticide Act (for example, maintaining rodent bait that is in use in covered, tamper-resistant bait stations)
  - knowing what poisonous and toxic chemicals should be on the premises and keeping track of them
  - investigating missing stock or other irregularities outside a normal range of variation and alerting local enforcement and public health agencies about unresolved problems, when appropriate

Operations

FDA recommends that retail food store and food service establishment operators consider:

- Incoming products

  - using only known and appropriately licensed or permitted (where applicable) sources for all incoming products
  - informing suppliers, distributors, and transporters about FDA's food security guidance, "Food Producers, Processors, and Transporters: Food Security Preventive Measures Guidance" and "Importers and Filers: Food Security Preventive Measures Guidance," available at: http://www.cfsan.fda.gov/~dms/guidance.html.
  - taking steps to ensure that delivery vehicles are appropriately secured
  - requesting that transporters have the capability to verify the location of the load at any time, when practical
  - establishing delivery schedules, not accepting unexplained, unscheduled deliveries or drivers, and investigating delayed or missed shipments
  - supervising off-loading of incoming materials, including off hour deliveries
  - reconciling the product and amount received with the product and amount ordered and the product and amount listed on the invoice and shipping documents, taking into account any sampling performed prior to receipt
  - investigating shipping documents with suspicious alterations
  - inspecting incoming products and product returns for signs of tampering, contamination, or damage (for example, abnormal powders, liquids, stains, or odors, evidence of resealing, compromised tamper-evident packaging) or "counterfeiting" (for example, inappropriate or mismatched product identity, labeling, product lot coding or specifications, absence of tamper-evident packaging when the label contains a tamper-evident notice), when appropriate
  - rejecting suspect food

- alerting appropriate law enforcement and public health authorities about evidence of tampering, "counterfeiting," or other malicious, criminal, or terrorist action

- Storage

  - having a system for receiving, storing, and handling distressed, damaged, and returned products, and products left at checkout counters, that minimizes their potential for being compromised (for example, obtaining the reason for return and requiring proof of identity of the individual returning the product, examining returned or abandoned items for signs of tampering, not reselling returned or abandoned products)
  - keeping track of incoming products, materials in use, salvage products, and returned products
  - investigating missing or extra stock or other irregularities outside a normal range of variability and reporting unresolved problems to appropriate law enforcement and public health authorities, when appropriate
  - minimizing reuse of containers, shipping packages, cartons, etc., where practical

- Food service and retail display

  - displaying poisonous and toxic chemicals for retail sale in a location where they can be easily monitored (for example, visible by staff at their work stations, windows, video monitoring)
  - periodically checking products displayed for retail sale for evidence of tampering or other malicious, criminal, or terrorist action (for example, checking for off-condition appearance [for example, stained, leaking, damaged packages, missing or mismatched labels], proper stock rotation, evidence of resealing, condition of tamper-evident packaging, where applicable, presence of empty food packaging or other debris on the shelving), to the extent practical
  - monitoring self-service areas (for example, salad bars, condiments, open bulk containers, produce display areas, doughnut/bagel cases) for evidence of tampering or other malicious, criminal, or terrorist action

- Security of water and utilities

  - Limiting, to the extent practical, access to controls for airflow, water, electricity, and refrigeration
  - securing non-municipal water wells, hydrants, storage, and handling facilities
  - ensuring that water systems and trucks are equipped with backflow prevention
  - chlorinating non-municipal water systems and monitoring chlorination equipment and chlorine levels
  - testing non-municipal sources for potability regularly, as well as randomly, and being alert to changes in the profile of the results
  - staying attentive to the potential for media alerts about public water provider problems, when applicable
  - identifying alternate sources of potable water for use during emergency situations where normal water systems have been compromised (for example, bottled water, trucking from an approved source, treating onsite or maintaining onsite storage)

- Mail/packages

  - implementing procedures to ensure the security of incoming mail and packages

- Access to computer systems

  - restricting access to critical computer data systems to those with appropriate clearance (for example, using passwords, firewalls)
  - eliminating computer access when a staff member is no longer associated with the establishment
  - establishing a system of traceability of computer transactions
  - reviewing the adequacy of virus protection systems and procedures for backing up critical computer-based data systems
  - validating the computer security system

Emergency Point of Contact:

U.S. Food and Drug Administration
5600 Fishers Lane
Rockville, MD 20857
301-443-1240

If a retail food store or food service establishment operator suspects that any of his/her products that are regulated by the FDA have been subject to tampering, "counterfeiting," or other malicious, criminal, or terrorist action, FDA recommends that he/she notify the FDA 24-hour emergency number at 301-443-1240 or call their local FDA District Office. FDA recommends that the operator also notify local law enforcement and public health authorities.

FDA District Office telephone numbers are listed at: http://www.fda.gov/ora/inspect_ref/iom/iomoradir.html.

---

*Reference to these documents is provided for informational purposes only. These documents are not incorporated by reference into this guidance and should not be considered to be FDA guidance.

The above document supercedes the previous version issued in March 2003.

U. S. Department of Health and Human Services
U. S. Food and Drug Administration
Center for Food Safety and Applied Nutrition
March 21, 2003

Guidance for Industry

Importers and Filers: Food Security Preventive Measures Guidance

This guidance represents the Agency's current thinking on the kinds of measures that food importers and filers may take to minimize the risk that food under their control will be subject to tampering or other malicious, criminal, or terrorist actions. It does not create or confer any rights for or on any person and does not operate to bind FDA or the public.

Purpose and Scope:

This guidance is designed as an aid to operators of food importing establishments, storage warehouses, and filers. It identifies the kinds of preventive measures that they may take to minimize the risk that food under their control will be subject to tampering or other malicious, criminal, or terrorist actions. Operators of food importing establishments are encouraged to review their current procedures and controls in light of the potential for tampering or other malicious, criminal, or terrorist actions and make appropriate improvements.

This guidance is designed to focus operator's attention sequentially on each segment of the food delivery system that is within their control, to minimize the risk of tampering or other malicious, criminal, or terrorist action at each segment. To be successful, implementing enhanced preventive measures requires the commitment of management and staff. Accordingly, FDA recommends that both management and staff participate in the development and review of such measures.

Limitations:

Not all of the guidance contained in this document may be appropriate or practical for every food importing establishment, particularly small facilities. FDA recommends that operators review the guidance in each section that relates to a component of their operation, and assess which preventive measures are suitable. Example approaches are provided for many of the preventive measures listed in this document. These examples should not be regarded as minimum standards. Nor should the examples provided be considered an inclusive list of all potential approaches to achieving the goal of the preventive measure. FDA recommends that operators consider the goal of the preventive measure, assess whether the goal is relevant to their operation, and, if it is, design an approach that is both efficient and effective to accomplish the goal under their conditions of operation.

Structure:

This guidance is divided into five sections that relate to individual components of food importing operations and practices: Management; Human Element -- Staff; Human Element -- Public; Facility; and Operations.

Related Guidance:

FDA has published a companion guidance document on food security, entitled, "Guidance for Food Producers, Processors, and Transporters: Food security preventive measures guidance". This document is available at: http://www.access.gpo.gov/su_docs/aces/aces140.html.

Additional Resources:*

A process called Operational Risk Management (ORM) may help prioritize the preventive measures that are most likely to have the greatest impact on reducing the risk of tampering or other malicious, criminal, or terrorist actions against food. Information on ORM is available in the Federal Aviation Administration (FAA) System Safety Handbook, U.S. Department of Transportation, FAA, December 30, 2000, Chapter 15, Operational Risk Management. The handbook is available at: http://www.asy.faa.gov/Risk/SSHandbook/Chap15_1200.PDF.

The U.S. Department of Transportation, Research and Special Programs Administration has published an advisory notice of voluntary measures to enhance the security of hazardous materials shipments. It is available at: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2002_register&docid=02-3636-filed.pdf. The notice provides guidance to shippers and carriers on personnel, facility and en route security issues.

The U.S. Postal Service has prepared guidance for identifying and handling suspicious mail. It is available at: http://www.usps.com/news/2001/press/mailsecurity/postcard.htm.

The Federal Anti-Tampering Act (18 USC 1365) makes it a federal crime to tamper with or taint a consumer product, or to attempt, threaten or conspire to tamper with or taint a consumer product, or make a false statement about having tampered with or tainted a consumer product. Conviction can lead to penalties of up to $100,000 in fines and up to life imprisonment. The Act is available at: http://www.fda.gov/opacom/laws/fedatact.htm.

The National Infrastructure Protection Center (NIPC) serves as the federal government's focal point for threat assessment, warning, investigation, and response for threats or attacks against U.S. critical infrastructure. The NIPC has identified the food system as one of the eight critical infrastructures, and has established a public-private partnership with the food industry, called the Food Industry Information and Analysis Center (Food Industry ISAC). The NIPC provides the Food Industry ISAC with access, information and analysis, enabling the food industry to report, identify, and reduce its vulnerabilities to malicious attacks, and to recover from such attacks as quickly as possible. In particular, the NIPC identifies credible threats and crafts specific warning messages to the food industry. Further information is available at http://www.nipc.gov/ and http://www.foodisac.org/.

Finally, FDA encourages trade associations to evaluate the preventive measures contained in this guidance document and adapt them to their specific products and operations and to supplement this guidance with additional preventive measures when appropriate. FDA welcomes dialogue on the content of sector specific guidance with appropriate trade associations.

Food Importing Operations

Management

FDA recommends that operators of food importing establishments consider:

Preparing for the possibility of tampering or other malicious, criminal, or terrorist actions

- assigning responsibility for security to knowledgeable individual(s)
- conducting an initial assessment of food security procedures and operations, which we recommend be kept confidential
- having a crisis management strategy to prepare for and respond to tampering and other malicious, criminal, or terrorist actions, both threats and actual events, including identifying, segregating and securing affected product
- planning for emergency evacuation, including preventing security breaches during evacuation
- becoming familiar with the emergency response system in the community
- making management aware of 24-hour contact information for local, state, and federal police/fire/rescue/health/homeland security agencies
- making staff aware of who in management they should alert about potential security problems (24-hour contacts)
- maintaining any floor and food flow plan in a secure, off-site location
- promoting food security awareness to encourage all staff to be alert to any signs of tampering or malicious, criminal, or terrorist actions or areas that may be vulnerable to such actions, and to report any findings to identified management (for example, providing training, instituting a system of rewards, building security into job performance standards)
- having an internal communication system to inform and update staff about relevant security issues
- having a strategy for communicating with the public (for example, identifying a media spokesperson, preparing generic press statements and background information, and coordinating press statements with appropriate authorities)

Supervision

- providing an appropriate level of supervision to all staff, including cleaning and maintenance staff, contract workers, data entry and computer support staff, and especially, new staff (for example, supervisor on duty, daily visits by supervisor, two staff on duty at all times, monitored video cameras, one way and two way windows)
- conducting routine security checks of the premises and critical computer data systems (at a frequency appropriate to the operation) for signs of tampering or malicious, criminal, or terrorist actions, or areas that may be vulnerable to such actions

Recall strategy

- identifying the person responsible, and a backup person
- providing for proper handling and disposition of recalled product
- identifying customer contacts, addresses, and phone numbers

Investigation of suspicious activity

- investigating threats or information about signs of tampering or other malicious, criminal, or terrorist actions
- alerting appropriate law enforcement and public health authorities about any threats of or suspected tampering or other malicious, criminal, or terrorist actions

Evaluation program

- evaluating the lessons learned from past tampering or other malicious, criminal, or terrorist actions and threats
- reviewing and verifying, at least annually, the effectiveness of the security management program (for example, using knowledgeable in-house or third party staff to conduct tampering or other malicious, criminal, or terrorist action exercises and mock recalls and to challenge computer security systems), revising the program accordingly, and keeping this information confidential
- performing random food security inspections of all appropriate areas of the facility (including receiving and storage, where applicable) using knowledgeable in-house or third party staff, and keeping this information confidential
- verifying that security contractors are doing an appropriate job, when applicable

Human element -- staff

Under Federal law, operators of food importing establishments are required to verify the employment eligibility of all new hires in accordance with the requirements of the Immigration and Nationality Act, by completing the INS Employment Eligibility Verification Form (INS Form I-9). Completion of Form I-9 for new hires is required by 8 USC 1324a and nondiscrimination provisions governing the verification process are set forth at 8 USC 1324b.

FDA recommends that operators of food importing establishments consider:

Screening (pre-hiring, at hiring, post-hiring)

- examining the background of all staff (including seasonal, temporary, contract, and volunteer staff, whether hired directly or through a recruitment firm) as appropriate to their position, considering candidates' access to sensitive areas of the facility and the degree to which they will be supervised and other relevant factors (for example, obtaining and verifying work references, addresses, and phone numbers, participating in one of the pilot programs managed by the Immigration and Naturalization Service and the Social Security Administration [These programs provide electronic confirmation of employment eligibility for newly hired employees. For more information call the INS SAVE Program toll free at 1-888-464-4218, fax a request for information to (202) 514-9981, or write to US/INS, SAVE Program, 425 I Street, NW, ULLICO-4th Floor, Washington, DC 20536. These pilot programs may not be available in all states], having a criminal background check performed by local law enforcement or by a contract service provider [Remember to first consult any state or local laws that may apply to the performance of such checks])

  Note: screening procedures should be applied equally to all employees, regardless of race, national origin, religion, and citizenship or immigration status.

Daily work assignments

- knowing who is and who should be on premises, and where they should be located, for each shift
- keeping assignment information updated

Identification

- establishing a system of positive identification and recognition that is appropriate to the nature of the workforce (for example, issuing uniforms, name tags, or photo identification badges, with individual control numbers, color coded by area of authorized access), when appropriate
- collecting the uniforms, name tag, or identification badge when a staff member is no longer associated with the establishment

Restricted access

- identifying staff that require unlimited access to all areas of the facility
- reassessing levels of access for all staff periodically
- limiting access so staff enter only those areas or have access to only those segments of the operation necessary for their job functions and only during appropriate work hours, including access to data operating systems for purchasing, storing and distributing imported foods (for example, using key card or keyed or cipher locks for entry to sensitive areas, color coded uniforms [remember to consult any relevant federal, state or local fire or occupational safety codes before making any changes])
- changing combinations, rekeying locks and/or collecting the retired key card when a staff member who is in possession of these is no longer associated with the establishment, and additionally as needed to maintain security

Personal items

- restricting the type of personal items allowed in non-public areas of the establishment
- allowing in the establishment only those personal use medicines that are necessary for the health of staff and ensuring that these personal use medicines are properly labeled and stored away from food handling or storage areas
- preventing staff from bringing personal items (for example, lunch containers, purses) into food preparation or storage areas
- providing for regular inspection of contents of staff lockers (for example, providing metal mesh lockers, company issued locks), bags, packages, and vehicles when on company property (Remember to first consult and federal, state, or local laws that may related to such inspections)

Training in food security procedures

- incorporating food security awareness, including information on how to prevent, detect, and respond to tampering or other malicious, criminal, or terrorist actions or threats, into training programs for staff, including seasonal, temporary, contract, and volunteer staff providing periodic reminders of the importance of security procedures (for example, scheduled meetings, providing brochures, payroll stuffers)
- providing periodic reminders of the importance of security procedures (for example, scheduled meetings, providing brochures, payroll stuffers)
- encouraging staff support (for example, involving staff in food security planning and the food security awareness program, demonstrating the importance of security procedures to the staff)

Unusual behavior

- watching for unusual or suspicious behavior by staff (for example, staff who, without an identifiable purpose, stay unusually late after the end of their shift, arrive unusually early, access files/information/areas of the facility outside of the areas of their responsibility; remove documents from the facility; ask questions on sensitive subjects; bring cameras to work)

Staff health

- being alert for atypical staff health conditions that staff may voluntarily report and absences that could be an early indicator of tampering or other malicious, criminal, or terrorist actions (for example, an unusual number of staff who work in the same part of the facility reporting similar symptoms within a short time frame), and reporting such conditions to local health authorities

Human element -- public

FDA recommends that operators of food importing establishments consider:

Visitors (for example, contractors, supplier representatives, delivery drivers, customers, couriers, pest control representatives, third-party auditors, regulators, reporters, tours)

- inspecting incoming and outgoing vehicles, packages and briefcases for suspicious, inappropriate or unusual items or activity, to the extent practical
- restricting entry to the establishment (for example, checking visitors in and out at security or reception, requiring proof of identity, issuing visitors badges that are collected upon departure, accompanying visitors)
- ensuring that there is a valid reason for the visit before providing access to the facility - beware of unsolicited visitors
- verifying the identity of unknown visitors
- restricting access to food handling and storage areas (for example, accompanying visitors, unless they are otherwise specifically authorized)
- restricting access to locker rooms

Facility

FDA recommends that operators of food importing establishments consider:

Physical security

- protecting perimeter access with fencing or other deterrent, when appropriate
- securing doors (including freight loading doors when not in use and not being monitored, and emergency exits), windows, roof openings/hatches, vent openings and trailer bodies, to the extent possible (for example, using locks, "jimmy plates," seals, alarms, intrusion detection sensors, guards, monitored video surveillance [remember to consult any relevant federal, state or local fire or occupational safety codes before making any changes])
- using metal or metal-clad exterior doors to the extent possible when the facility is not in operation, except where visibility from public thoroughfares is an intended deterrent (remember to consult any relevant federal, state or local fire or occupational safety codes before making any changes)
- securing bulk unloading equipment (for example, augers, pipes, conveyor belts, and hoses) when not in use and inspecting the equipment before use
- minimizing the number of entrances to restricted areas (remember to consult any relevant federal, state or local fire or occupational safety codes before making any changes)
- accounting for all keys to establishment (for example, assigning responsibility for issuing, tracking and retrieving keys)
- monitoring the security of the premises using appropriate methods (for example, using security patrols [uniformed and/or plain-clothed] and video surveillance)
- minimizing to the extent practical, places that can be used to temporarily hide intentional contaminants (for example, minimizing nooks and crannies, false ceilings)
- providing adequate interior and exterior lighting, including emergency lighting, where appropriate, to facilitate detection of suspicious or unusual activity
- implementing a system of controlling vehicles authorized to park on the premises (for example, using placards, decals, key cards, keyed or cipher locks, issuing passes for specific areas and times to visitors' vehicles)
- keeping parking areas separated from entrances to food storage and processing areas and utilities, where practical

Storage and use of poisonous and toxic chemicals (for example, cleaning and sanitizing agents, pesticides)

- limiting poisonous and toxic chemicals in the establishment to those that are required for the operation and maintenance of the facility and those that are being held for sale
- storing poisonous and toxic chemicals as far away from food handling and storage areas as practical
- limiting access to and securing storage areas for poisonous and toxic chemicals that are not being held for sale (for example, using keyed or cipher locks, keycards, seals, alarms, intrusion detection sensors, guards, monitored video surveillance [remember to consult any relevant state or local fire codes before making any changes])
- ensuring that poisonous and toxic chemicals are properly labeled
- using pesticides in accordance with the Federal Insecticide, Fungicide, and Rodenticide Act (for example, maintaining rodent bait that is in use in covered, tamper-resistant bait stations)
- knowing what poisonous and toxic chemicals should be on the premises and keeping track of them
- investigating missing stock or other irregularities outside a normal range of variation and alerting appropriate law enforcement and public health authorities about unresolved problems, when appropriate

Operations

FDA recommends that operators of food importing establishments consider:

Incoming products

- using only known and appropriately licensed or permitted (where applicable) sources for all products
- taking reasonable steps to encourage suppliers, distributors and transporters to practice appropriate food security measures (for example, auditing, where practical, for compliance with food security measures that are contained in purchase and shipping contracts or letters of credit or using a vendor approval program.)
- authenticating labeling, packaging configuration, tamper-evident packaging and product coding/expiration dating systems (where applicable) in advance of receipt of shipment, especially for new products
- requesting locked and/or sealed vehicles/containers/railcars, and, if sealed, obtaining the seal number from the supplier, and verifying upon receipt, making arrangements to maintain the chain of custody when a seal is broken for inspection by a governmental agency or as a result of multiple deliveries
- requesting that transporters have the capability to verify the location of the load at any time, when practical
- establishing delivery schedules, not accepting unexplained, unscheduled deliveries or drivers, and investigating delayed or missed shipments
- supervising off-loading of incoming materials, including off hour deliveries
- reconciling the product and amount received with the product and amount ordered and the product and amount listed on the invoice and shipping documents, taking into account any sampling performed prior to receipt
- investigating shipping documents with suspicious alterations
- inspecting incoming products and product returns for signs of tampering, contamination or damage (for example, abnormal powders, liquids, stains, or odors, evidence of resealing, compromised tamper-evident packaging) or "counterfeiting" (inappropriate or mismatched product identity, labeling, product lot coding or specifications, absence of tamper-evident packaging when the label contains a tamper-evident notice), when appropriate
- inspecting incoming products for authenticity, packaging/product integrity, and evidence of unauthorized relabeling/repackaging (for example, shipping cases and described contents not consistent with actual contents) and verifying batch/lot/container codes
- verifying conformance with FDA requirements for product safety, quality, effectiveness, and labeling (may require contact with and verification from the foreign manufacturer/processor)
- evaluating the utility of testing incoming products and product returns for detecting tampering or other malicious, criminal, or terrorist action
- developing and implementing procedures for inspecting shipping containers, vehicles
- investigating damage and loss and alerting appropriate authority of discrepancies
- rejecting suspect food
- alerting appropriate law enforcement and food public health authorities about evidence of tampering, "counterfeiting" or other malicious, criminal, or terrorist action

Storage

- having a system for receiving, storing and handling distressed, damaged, returned, and reworked products that minimizes their potential for being compromised or to compromise the security of other products (for example, destroying products that are unfit for human or animal consumption, products with illegible codes, products or questionable origin, and products returned by consumers to retail stores)
- keeping track of incoming products, salvage products, and returned products
- minimizing reuse of containers, shipping packages, cartons, etc., where practical
- investigating missing or extra stock or other irregularities outside a normal range of variability and reporting unresolved problems to appropriate law enforcement and public health agencies, when appropriate

Outgoing products

- ensuring that public storage warehousing and shipping (vehicles and vessels) practice appropriate security measures (for example, auditing for compliance with food security measures that are contained in contracts or letters of guarantee
- performing random inspection of storage facilities, vehicles, and vessels
- requesting locked and/or sealed vehicles/containers/railcars and providing the seal number to the consignee (remember to consult any relevant federal, state or local fire or occupational safety codes before making any changes)
- establishing scheduled pickups and not accepting unexplained, unscheduled pickups
- restricting access to distribution process to employees with appropriate clearance
- requesting that the transporter have the capability to verify the location of the load at any time
- advising sales staff to be on the lookout for counterfeit products during visits to customers and notify management if any problems are detected
- investigating missing or extra stock or other irregularities outside a normal range of variation and alerting appropriate law enforcement and public health authorities about unresolved problems, when appropriate

Security of water and utilities

- limiting, to the extent practical, access to controls for airflow, water, electricity, and refrigeration securing non-municipal water wells, hydrants, storage, and handling facilities
- ensuring that water systems and trucks are equipped with backflow prevention
- chlorinating water systems and monitoring chlorination equipment, where practical, and especially for non-municipal water systems
- testing non-municipal sources for potability regularly, as well as randomly, and being alert to changes in the profile of the results
- staying attentive to the potential for media alerts about public water provider problems, when applicable
- identifying alternate sources of potable water for use during emergency situations where normal water systems have been compromised (for example, bottled water, trucking from an approved source, treating on-site or maintaining on-site storage)

Security of ventilation system (where applicable)

- securing access to air intake points for the facility, to the extent possible (for example, using fences, sensors, guards, video surveillance)
- examining air intake points for physical integrity routinely

Mail/packages

- implementing procedures to ensure the security of incoming mail and packages (for example, following U.S. Postal Service guidance, locating the mailroom away from food handling and storage areas, securing mailroom visual or x-ray mail /package screening,)

Access to computer systems

- restricting access to critical computer data systems to those with appropriate clearance (for example, using

passwords, firewalls)
- eliminating computer access when a staff member is no longer associated with the establishment
- establishing a system of traceability of computer transactions
- reviewing the adequacy of virus protection systems and procedures for backing up critical computer based data systems
- validating and periodically challenging the computer security system and procedures

Emergency Point of Contact:

U.S. Food and Drug Administration
5600 Fishers Lane
Rockville, MD 20857

If a food import establishment operator suspects that any of his/her products that are regulated by the FDA have been subject to tampering, "counterfeiting", or other malicious, criminal, or terrorist action, FDA recommends that he/she notify the FDA 24-hour emergency number at 301-443-1240 or call their local FDA District Office. FDA District Office telephone numbers are listed at http://www.fda.gov/ora/inspect_ref/iom/iomoradir.html. FDA recommends that the operator also notify local law enforcement and public health agencies.

---

* Reference to these documents is provided for informational purposes only. These documents are not incorporated by reference into this guidance and should not be considered to be FDA guidance.

July 11, 2003

Guidance for Industry

Dairy Farms, Bulk Milk Transporters, Bulk Milk Transfer Stations and Fluid Milk Processors Food Security Preventive Measures Guidance

FINAL GUIDANCE

Comments regarding this document may be submitted at any time to the Division of Dockets Management (HFA-305), Food and Drug Administration, 5630 Fishers Lane, rm. 1061, Rockville, MD 20852. Submit electronic comments to http://www.fda.gov/dockets/ecomments.

For questions regarding this document, contact John Kvenberg, Office of Compliance, HFS-600, Center for Food Safety and Applied Nutrition (CFSAN), Food and Drug Administration, 5100 Paint Branch Pkwy., College Park, MD 20740, 301-436-2359, e-mail: jkvenberg@cfsan.fda.gov or Donald W. Kraemer, Office of Seafood (HFS-400), Center for Food Safety and Applied Nutrition (CFSAN), Food and Drug Administration, 5100 Paint Branch Pkwy., College Park, MD 20740, 301-436-2300, e-mail: dkraemer@cfsan.fda.gov.

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Food Safety and Applied Nutrition
July 2003

Guidance for Industry

Dairy Farms, Bulk Milk Transporters, Bulk Milk Transfer Stations and Fluid Milk Processors Food Security Preventive Measures Guidance

This guidance represents FDA's current thinking on the kinds of measures that operators of dairy farms, bulk milk transportation operations, bulk milk transfer stations, and fluid milk processing facilities may take to minimize the risk that fluid milk under their control will be subject to tampering or other malicious, criminal, or terrorist actions. It does not create or confer any rights for or on any person and does not operate to bind FDA or the public. If you want to discuss an alternative approach, contact the FDA staff responsible for implementing this guidance. If you cannot identify the appropriate FDA staff, call the telephone number listed on the title page of this guidance.

Purpose, Scope and Limitations:

This guidance is designed as an aid to operators of dairy farms, bulk milk transportation operations, bulk milk transfer stations and fluid milk processing facilities. It identifies the kinds of preventive measures operators of these establishments may take to minimize the risk that fluid milk under their control will be subject to tampering or other malicious, criminal, or terrorist actions. Operators of these establishments are encouraged to review their current procedures and controls in light of the potential for tampering or other malicious, criminal, or terrorist actions and make appropriate improvements.

FDA's guidance documents, including this guidance, do not establish legally enforceable responsibilities. Instead guidances describe the Agency's current thinking on a topic and should be viewed only as recommendations, unless specific regulatory or statutory requirements are cited. The use of the word *should* in Agency guidances means that something is suggested or recommended, but not required.

Not all of the guidance contained in this document may be appropriate or practical for every dairy farm, bulk milk transportation operation, bulk milk transfer station, or fluid milk processing facility. FDA recommends that operators of these establishments review the guidance in each section that relates to a component of their operation, and assess which preventive measures are suitable. FDA further recommends that operators consider the goal of the preventive measure, assess whether the goal is relevant to their operation, and, if it is, design an approach that is both efficient and effective to accomplish the goal under their conditions of operation.

Additional food security guidance that may also be applicable to operators of these establishments is contained in an FDA guidance document entitled, "Food Producers, Processors, and Transporters: Food Security Preventive Measures Guidance." This document is available at: http://www.cfsan.fda.gov/~dms/secguid6.html.

Management

FDA recommends that operators of dairy farms, bulk milk transportation operations, bulk milk transfer stations and fluid milk processing facilities consider:

- Conducting an initial assessment of the adequacy of food security procedures and operations, which we recommend be kept confidential.
- Developing a security management strategy to prepare for and respond to tampering and other malicious, criminal or terrorist actions, both threats and actual events, including identifying, segregating and securing affected product.
- Developing a product recall strategy
- Providing training in food security awareness to encourage all staff to be alert to any signs of tampering or other malicious, criminal or terrorist actions or areas that may be vulnerable to such actions, and report any findings to management. The training may also encourage staff to be alert to the presence of unidentified or unknown individuals or individuals that are in areas to which they are not designated access, and to directly question such individuals or report them to management
- Providing appropriate supervision to all staff with access to raw and pasteurized milk storage, vitamin supplement receiving and storage, and milk processing and packaging areas of the facility, including cleaning, maintenance and quality control staff, seasonal, temporary, contract, and volunteer staff, and especially, new staff. The supervision may include watching for unusual or suspicious behavior by staff (e.g., staff who, without an identifiable purpose, stay unusually late after the end of their shift, arrive unusually early, access files/information/areas of the facility outside of the areas of their responsibility; remove documents from the facility; ask questions on sensitive subjects; bring cameras to work)
- Conducting routine security checks of the raw and pasteurized milk storage, vitamin supplement receiving and storage, and milk processing and packaging areas of the facility, for signs of tampering or malicious, criminal or terrorist actions or areas that may be vulnerable to such actions.
- Alerting appropriate law enforcement and public health authorities about any threats of or suspected tampering or other malicious, criminal or terrorist actions. FDA may be contacted through its 24-hour emergency number, 301-443-1240, or through a local FDA District Office. FDA District Office telephone numbers are listed at: http://www.fda.gov/ora/inspect_ref/iom/iomoradir.html.
- Reviewing, at least annually, the effectiveness of the food security plan, using knowledgeable in-house or third party staff, and revising the program accordingly, which we recommend be kept confidential.

Human element

FDA recommends that operators of dairy farms, bulk milk transportation operations, bulk milk transfer stations and fluid milk processing facilities consider:

- Obtaining and verifying work references, addresses and phone numbers of all staff with access to raw and pasteurized milk storage, vitamin supplement receiving and storage, and milk processing and packaging areas of the facility, including cleaning, maintenance and quality control staff, seasonal, temporary, contract, and volunteer staff.
- Having a criminal background check performed by local law enforcement or by a contract service provider for the above listed staff, except if such staff are under direct supervision when they access the above listed areas.
- Limiting access to raw and pasteurized milk storage, vitamin supplement receiving and storage, and milk processing and packaging areas of the facility to those staff that need to enter because of their job functions and only during appropriate work hours.
- Preventing staff from bringing personal items (e.g., lunch containers, purses) into raw and pasteurized milk storage, vitamin supplement receiving and storage, and milk processing and packaging areas of the facility.
- Being alert for atypical staff health conditions that staff may voluntarily report and absences that could be an early indicator of tampering or other malicious, criminal or terrorist actions (e.g., an unusual number of staff who work in the same part of the facility reporting similar symptoms within a short time frame), and reporting such conditions to local health authorities
- Accompanying all visitors.

Facility

FDA recommends that operators of dairy farms, bulk milk transportation operations, bulk milk transfer stations and fluid milk processing facilities consider:

- Securing doors (including freight loading doors, when not in use and not being monitored, and emergency exits), windows, roof openings/hatches, vent openings, ventilation systems, utility rooms, loft areas, trailer bodies, tanker trucks, and bulk storage tanks, to the extent possible.
- Inspecting bulk unloading equipment and pumps in the receiving area before use.
- Monitoring the security of the premises.

FDA further recommends that operators of dairy farms consider:

- Locking or sealing, with serially numbered seals, all entrances to the milk house or all entry ports on the bulk milk tank from the time the bulk milk tank is washed until the time it is emptied, except when it is under direct, visual supervision (Remember to first make arrangements with the State regulatory agency that will ensure that the regulatory agency, rating agency and FDA continue to have ready access to the milk house and milking operation for routine inspections, Grade "A" IMS ratings and FDA check ratings, when applicable).

Operations

Vitamin supplements and laboratory supplies

FDA recommends that operators of fluid milk processing facilities consider:

- Using only known, appropriately licensed or permitted (where applicable) sources for vitamin supplements.
- Establishing delivery schedules for vitamin supplements, not accepting unexplained, unscheduled deliveries or drivers, and investigating delayed or missed shipments.
- Supervising off-loading of incoming vitamin supplements, laboratory reagents and positive controls, including off-hour deliveries.
- Reconciling the product and amount received with the product and amount ordered and the product and amount listed on the invoice and shipping documents.
- Investigating shipping documents with suspicious alterations.
- Inspecting incoming vitamin supplements for signs of tampering, contamination or damage (e.g., abnormal powders, liquids, stains, or odors, evidence of resealing) or "counterfeiting" (e.g., inappropriate or mismatched product identity, labeling, product lot coding or specifications).
- Storing vitamin supplements, laboratory reagents, and positive controls in a secure location.
- Keep track of vitamin supplements, laboratory reagents and positive controls and investigating any missing or extra stock outside a predetermined normal range of variability.

Labeling

FDA recommends that operators of fluid milk processing facilities consider:

- Storing product labels in a secure location and destroying outdated or discarded labels

Raw milk

FDA recommends that operators of bulk milk transfer stations and fluid milk processing facilities consider:

- Accepting only those incoming tanker loads of raw milk for which all openings were either locked or sealed, with a serially numbered seal, from the time the tanker was last washed until the load is delivered. Exception may be provided for incoming loads for which a thorough investigation demonstrates that there is a verified, reasonable explanation for a deviation. Seals or locks need not be in place during those times that the tanker was under the direct, visual supervision of the driver.
- Using only known, reputable transportation companies
- Establishing delivery schedules for raw milk, not accepting unexplained, unscheduled deliveries or drivers, and investigating delayed or missed shipments. We recommend that driver identification include the name of the transportation company.
- Supervising off-loading of incoming milk.
- Reconciling the amount received with the amount listed on the shipping documents.
- Verifying that operators of bulk milk transfer stations that supply raw milk adhere to the preventive measures listed in this guidance.

FDA recommends that operators of bulk milk transportation operations consider:

- Locking or sealing, with a serially numbered seals, every tanker from the time it is last washed until the time the load of milk is delivered to the bulk milk transfer station or fluid milk processing facility. Seals or locks need not be in place during those times that the tanker is under the direct, visual supervision of the driver.

Analyzing a bioterror attack on the food supply: The case of botulinum toxin in milk

Lawrence M. Wein*† and Yifan Liu‡

*Graduate School of Business and ‡Institute for Computational and Mathematical Engineering, Stanford University, Stanford, CA 94305

Edited by Barry R. Bloom, Harvard University, Boston, MA, and approved April 20, 2005 (received for review November 16, 2004)

We developed a mathematical model of a cows-to-consumers supply chain associated with a single milk-processing facility that is the victim of a deliberate release of botulinum toxin. Because centralized storage and processing lead to substantial dilution of the toxin, a minimum amount of toxin is required for the release to do damage. Irreducible uncertainties regarding the dose–response curve prevent us from quantifying the minimum effective release. However, if terrorists can obtain enough toxin, and this may well be possible, then rapid distribution and consumption result in several hundred thousand poisoned individuals if detection from early symptomatics is not timely. Timely and specific in-process testing has the potential to eliminate the threat of this scenario at a cost of <1 cent per gallon and should be pursued aggressively. Investigation of improving the toxin inactivation rate of heat pasteurization without sacrificing taste or nutrition is warranted.

bioterrorism | mathematical modeling

Among bioterror attacks not involving genetic engineering, the three scenarios that arguably pose the greatest threats to humans are a smallpox attack, an airborne anthrax attack, and a release of botulinum toxin in cold drinks (1). The methods of dissemination in these three scenarios are, respectively, the person-to-person spread of a contagious disease, the outdoor dispersal of a highly durable and lethal agent, and the large-scale storage and production and rapid widespread distribution and consumption of beverages containing the most poisonous substance known. The first two scenarios have been the subject of recent systems modeling studies (2–5), and here we present a detailed systems analysis of the third scenario. For concreteness, we consider a release in the milk supply, which, in addition to its symbolic value as a target, is characterized by the rapid distribution of 20 billion gallons per year in the U.S.; indeed, two natural *Salmonella* outbreaks in the dairy industry each infected ≈200,000 people (6). Nonetheless, our methods are applicable to similar food products, such as fruit and vegetable juices, canned foods (e.g., processed tomato products), and perhaps grain-based and other foods possessing the bow-tie-shaped supply chain pictured in Fig. 1.

The Model

The mathematical model considers the flow of milk through a nine-stage cows-to-consumers supply chain associated with a single milk-processing facility (Fig. 1). *Supporting Appendix*, which is published as supporting information on the PNAS web site, contains a detailed mathematical formulation of the model, a discussion of the modeling assumptions, and the specification of parameter values, some of which are listed in Table 1. The supply-chain parameter values are representative of the California dairy industry, which produces >20% of the nation's milk (California dairy facts, www.dairyforum.org/cdf.html, accessed on May 18, 2004). In our model, cows are milked twice daily, and the milk from each farm is picked up once per day by a 5,500-gallon truck, which makes two round trips daily between various farms and the processing plant. Upon a truck's arrival at the processing plant, the milk is piped into one of several raw milk silos, each capable of holding ≈50,000 gallons. Raw milk is piped into the processing facility, goes through a sequence of processes (e.g., separation, pasteurization, homogenization, and vitamin fortification), where each processing line may simultaneously receive milk from several silos, and is held in 10,000-gallon postpasteurization tanks before being bottled. In our base case, we assume that milk from different silos does not mix during downstream processing and relax this assumption later; although downstream mixing is physically possible at many facilities, it is not always done. Bottled milk is stored as finished-goods inventory before traveling through the downstream distribution channel, eventually being purchased and consumed.

We assume that botulinum toxin is deliberately released in either a holding tank at a dairy farm, a tanker truck transporting milk from a farm to the processing plant, or a raw milk silo at the processing facility. Each of these release locations leads to identical consequences, because the toxin is eventually well mixed throughout the contents of a raw milk silo. The crux of our analysis is to calculate the amount and toxin concentration of contaminated milk (see Fig. 4, which is published as supporting information on the PNAS web site). By California state law, a raw milk silo must be cleaned after 72 h of operation. During these 72 h, the silo is initially filled up, then replenished (i.e., simultaneously filled and drained) for most of the 72-h period, and finally drained empty by 72 h. Because the toxin concentration in the silo drops exponentially during the replenishment interval, each postpasteurization holding tank has a different concentration level. Moreover, the amount of contaminated milk and the concentration distribution are themselves random quantities, depending upon when in the 72-h silo operation cycle the deliberate release occurs. Because of the difficulty of a terrorist in scheduling the release for maximum impact, we assume the release occurs randomly throughout the filling and replenishment intervals and report the mean number of poisoned people averaged over the random release time within the cycle. Using heat-inactivation data for foods with similar pH (7), we estimate that the heat-pasteurization process [170°F (77°C) for 15 min] inactivates 68.4% of the toxin.

Each gallon of purchased milk is continuously consumed by four people (one child and three adults) over a 3.5-day period. Children aged 2–11 and adults have differential milk consumption rates and dose–response curves in our model. A probit dose–response model dictates the precise timing of each poisoning. Our dose–response relationship is based on scant human data (ID_{50} = 1 μg for adults, ID_{50} = 0.43 μg for children) (8, 9). The attack can be detected via either early symptomatics or in-process testing results, whichever occurs first. We assume the outbreak is detected when the 100th person develops symptoms [the incubation period, which is the interval between the time of poisoning and the onset of symptoms, is log normal with a median of 48 h and a dispersal factor of 1.5 (10)], and an additional 24 h are required to identify the attack as being milkborne, at which time all consumption is halted. As with current antibiotic residue testing, we assume in-process botulinum testing is performed on milk from each truck just before the milk is piped into a raw milk silo at the processing facility. We have two tests at our disposal: the Food and Drug Administration-approved mouse assay with a detection limit of 16 pg/ml (11) and a testing delay of 48 h, and an ELISA test with a detection limit of 80 pg/ml (12) and a testing delay of 3 h. Because the mouse assay is not practical for widespread use (assays are processed at only several U.S. laboratories, and the mouse supply is limited), we assess two strategies: the ELISA test used in isolation (i.e., consumption is stopped after a positive ELISA result) and a sequential strategy in which the mouse assay is used as a confirmatory test after a positive ELISA result (i.e., consumption is halted after a positive mouse result). The latter strategy has a detection limit of 80 pg/ml and a testing delay of 51 h. The ELISA test in isolation is practical only if the test has an extremely small false-positive rate (no data have been published on ELISA test specificity in milk); otherwise, the sequential strategy is the only viable alternative.

This paper was submitted directly (Track II) to the PNAS office.

Freely available online through the PNAS open access option.

†To whom correspondence should be addressed. E-mail: lwein@stanford.edu.

www.pnas.org/cgi/doi/10.1073/pnas.0408526102

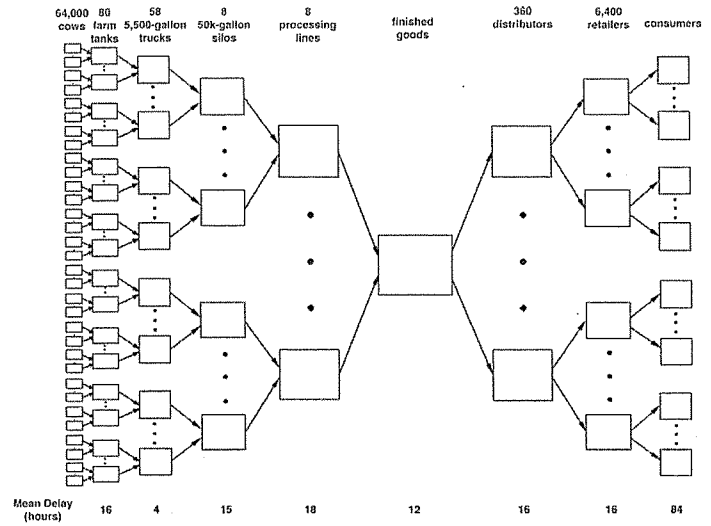


Fig. 1. The milk supply chain.

Results

In the absence of any detection (i.e., every gallon of contaminated milk is consumed), the mean number of people who consume contaminated milk is 568,000 (Fig. 2) Less than 1 g of toxin is required to cause 100,000 mean casualties (i.e., poisoned individuals), and 10 g poison the great majority of the 568,000 consumers (Fig. 2). Most of the casualties occur on days 3–6, although they happen somewhat faster for larger releases, because less consumption is required for poisoning. Due to children's higher consumption rate and greater toxin sensitivity, the percentage of casualties who are children in Fig. 2 decreases from 99.97% for a 0.1-g release, to 61% for a 1-g release, to 28% for a 10-g release.

Early symptomatic detection avoids ≈2/3 of the casualties in Fig. 2 (see Fig. 3) but still allows >100,000 mean casualties for a release of 10 g. Relative to no testing, the sequential testing strategy cuts the number poisoned approximately in half, resulting in tens of thousands of cases. The ELISA testing strategy used in isolation prevents nearly all cases, e.g., if 1 kg is released then the mean number poisoned is 2.82, and six people are poisoned even if the terrorist chooses the worst-case release time within the silo cleaning cycle.

Table 2 contains the results of a sensitivity analysis of isolated changes in 10 key parameters in the no-testing case. Five of these 10 changes impact the number of casualties in the no-detection case (Table 3). Graphs corresponding to Tables 2 and 3 appear in *Supporting Appendix*. The first 4 of these 10 changes involve milk storage and processing. Reducing the time between silo cleanings from 72 to 48 h lowers the number poisoned by ≈30% in a large attack with no detection but otherwise has a modest impact. Increasing the silo size from 50,000 to 100,000 gallons (several raw milk silos in California hold up to 200,000 gallons), while varying the number of silos so that the total silo capacity is fixed at 400,000 gallons, and maintaining a dedicated processing line for each silo leads to slightly fewer casualties for small releases but up to twice as many poisoned for large releases and no detection. Similarly, allowing milk from four silos to mix during downstream processing can quadruple the number of casualties in a large attack with no detection. Because the toxin inactivation rate may be very sensitive to the pasteurization temperature and time in the neighborhood of the current pasteurization formula (7), we consider a pasteurization process that causes a 2-log reduction in active toxin. This leads to a huge reduction in casualties if the release size is 10 g or less but has no impact for a 1-kg release.

The remaining six changes are from the downstream portion of the supply chain. We could not find reliable data on the speed of the distribution channel. More rapid distribution leads to

Table 1. Base-case values for model parameters

Parameter description	Value
Production rate	10 gallons per cow per day
Silo size	50,000 gallons
Silos per processing line	1
Time between silo cleanings	72 hr
Speed of distribution channel	80% of milk purchased within 48 hr
Consumers per gallon of milk	4
Time to consume 1 gallon of milk	84 hr
Dose–response probit slope	4.34
Adult ID_{50}	1 μg
Child ID_{50}	0.43 μg
Median incubation (adult and child)	48 hr
Dispersal factor of incubation	1.5
Number of symptomatics until detection	100
Time to detect attack is milkborne	24 hr
Testing-detection limit (mouse, ELISA)	60.6 ng/gallon, 303 ng/gallon
Testing-time delay (mouse, ELISA)	48 hr, 3 hr
Fraction of toxin not inactivated by pasteurization	0.316
Fraction of milk consumers who are children	0.25
Fraction of milk consumed by children	0.4

earlier consumption and faster diagnosis, and the former effect appears to dominate, leading to larger attack sizes. Our base-case value for the time to drink a gallon of milk is based on the conservative assumption that everyone has the same consumption rate. However, there is considerable heterogeneity in consumption rates across the population, which causes heavier consumers to buy milk more frequently. Hence, we assume it takes 24 rather than 84 h for a gallon to be consumed. As in the case of rapid distribution, a higher consumption rate leads to more casualties. The dose–response data in Tables 2 and 3 are based on monkey data, which are more plentiful than human data. As in the pasteurization case, the monkey data lead to a drastic reduction in casualties for a small release but have little effect in a large release. Because children rarely eat in restaurants or eat home-canned food, nearly all of the historical incubation data are based on adults. We assume that the median

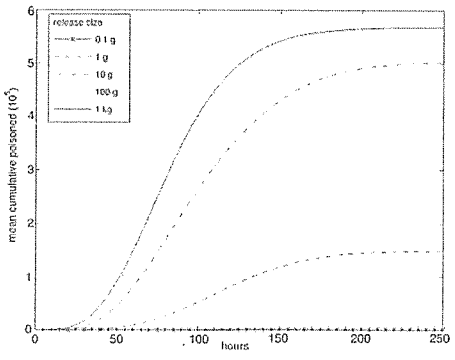


Fig. 2. The mean cumulative number of people poisoned over time for various release sizes in the absence of any detection.

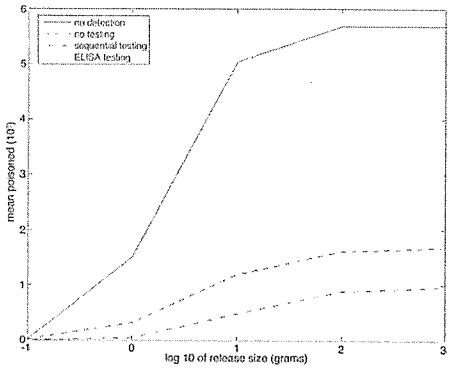


Fig. 3. The mean total number of people poisoned vs. release size for various detection scenarios.

incubation time for children is reduced from 48 to 12 h because of their smaller mass and larger consumption of tainted milk, which lead to earlier detection and many fewer casualties. Our last two changes relate to detection time. The Centers for Disease Control and Prevention maintains a well established national surveillance system for botulism (14) that has been enhanced in the last several years. Botulism in virtually all jurisdictions is an immediately reportable disease, and the characteristic clinical features of botulism suggest that the outbreak might be recognized promptly (e.g., by the presentation of the 10th case). Moreover, because most metropolitan areas have only one or two children's hospitals, and because milk is one of the few staples in children's diets, the time to detect the outbreak as milkborne might be rather quick (e.g., 12 h). Not surprisingly, both changes lead to a reduction in the number of people poisoned.

Discussion

Combating bioterrorism requires an appropriate mix of prevention, mitigation, detection, and response. Our observation that, due to the successive mixing operations in the upstream portion of the supply chain, the impact of a deliberate release upstream of the processing plant is independent of the precise location may aid in prioritizing resources for prevention. A foodborne attack is much more preventable than an airborne or mailborne attack, due to the restricted number of release locations. Requiring all tanks, trucks, and silos to be locked when not being drained or filled would be an obvious step forward, as would security checks for personnel who have access to prebottled milk (farm laborers, truck drivers, receiving labor at the processing facility, and plant engineers) and requiring one person from each stage of the supply chain to be present while milk is transferred from one stage to the next (15). Although these and other measures are included in proposed Food and Drug Administration guidelines (16), they are currently voluntary. Homeland security officials need to engage industry leaders to establish the most appropriate way to guarantee these guidelines are enforced. Although enforcement options range from voluntary guidelines to new laws, the most promising approach may be to develop International Organization for Standardization (ISO) security standards that are analogous to the ISO 9000 standards for quality management and the ISO 14000 standards for environmental

Table 2. Sensitivity analysis for 10 parameters in the no-testing case

Case description	Release size 0.1 g	1 g	10 g	100 g	1 kg
Base case	1.7×10^3	3.2×10^4	1.2×10^5	1.6×10^5	1.7×10^5
Time between silo cleanings = 48 hr	2.0×10^3	3.5×10^4	1.2×10^5	1.5×10^5	1.5×10^5
Silo size = 100,000 gallons	2.1×10^2	3.2×10^4	1.6×10^5	2.7×10^5	3.0×10^5
Silos per processing line = 4	4.4×10^1	2.7×10^4	1.9×10^5	4.5×10^5	5.3×10^5
Inactivation by pasteurization = 0.99	6.6×10^{-11}	5.0	1.3×10^4	7.3×10^4	1.5×10^5
Distribution: 90% purchased ≤ 24 hr	2.0×10^3	4.5×10^4	1.8×10^5	2.4×10^5	2.6×10^5
Time to consume a gallon = 24 hr	1.9×10^3	6.2×10^4	1.5×10^5	1.7×10^5	1.7×10^5
ID_{50} (adult, child) = 70 μg, 30 μg	1.8×10^{-16}	6.7×10^{-3}	4.3×10^3	4.2×10^4	1.3×10^5
Median child incubation = 12 hr	6.4×10^2	7.5×10^3	3.4×10^4	5.6×10^4	6.0×10^4
Symptomatics until detection = 10	1.1×10^3	2.0×10^4	8.4×10^4	1.2×10^5	1.2×10^5
Milkborne detection time = 12 hr	1.5×10^3	2.0×10^4	6.9×10^4	9.3×10^4	9.6×10^4

Each change from the base-case value in Table 1 was made in isolation and shown are the mean number of poisoned people computed for five different release sizes.

management (www.iso.ch/iso/en/iso9000–14000/index.html, accessed on November 12, 2004).

Turning to mitigation, botulinum toxin cannot be completely inactivated by radiation (17) or any heat treatment that does not adversely affect the milk's taste. Ultrahigh-temperature (UHT) pasteurization (performed to provide extended shelf life) appears capable of completely inactivating botulinum toxin in milk, but UHT milk has not been embraced by U.S. consumers. Nonetheless, it is worthwhile to perform pasteurization studies to determine whether a more potent inactivation process can be used without compromising nutrition or taste, particularly because the inactivation rate appears to be quite sensitive to the pasteurization temperature and time in the neighborhood of the current pasteurization formula (7). Reducing the time between silo cleanings decreases the number of people poisoned in, at most, a linear manner, but more frequent cleanings would not only increase variable material and labor costs but would possibly require fixed investments in additional silos.

Before discussing detection, we note that, on the response side, ≈60% of poisoned individuals would require mechanical ventilation (6). Given the small number of ventilators and limited amount of antitoxin in the national stockpile, the death rate from a large attack would likely be closer to the pre-1950s 60% rate (18) or the 25% rate incurred in the 1950s than to the 6% death rate experienced in the 1990s (19). Moreover, the current treatment, a passive immunization with equine antitoxin, does not reverse existent paralysis, and postexposure prophylaxis with antitoxin has adverse side effects (19). Although an economic impact assessment of this scenario is beyond the scope of our study, the economic cost (including direct medical costs and lost productivity due to illness and death) from a hypothetical botulism outbreak that poisons 50,000 people was estimated to be 8.6 billion (20), using a direct medical cost (assuming ample ventilators and antitoxin) per hospitalized patient of ≈$55,000 (based on Canadian dollars in 1993–1994). In contrast, two recent U.S. victims receiving injections of "fake Botox" each incurred a $350,000 medical bill in the first 2 weeks of illness [S. Z. Grossman (lawyer of Botox victims), personal communication]. If this latter amount was spent on each survivor in an attack that poisoned several hundred thousand people, then the total medical costs would be tens of billions of dollars.

Our study highlights the value of rapid in-process testing for detecting an attack, and because stockpiling sufficient ventilators and antitoxin in the event of a large-scale attack would be exorbitantly expensive, it seems wise to aggressively invest in rapid, sensitive, and specific in-process testing. A variety of different botulinum testing technologies are being investigated as alternatives to the mouse assay [summary of the National Institute of Allergy and Infectious Diseases (NIAID) expert panel on botulinum diagnostics, May 23, 2003, www2.niaid.nih.gov/NR/rdonlyres/BB1DDC43-1906-4450-8983-DB0BE3744746/0/bottoxinsmtg.pdf, accessed on November 15, 2004], although published data exist only for the ELISA assay. The current ELISA test appears to be ≈2 orders of magnitude more sensitive than needed: if milk in a truck contains 300 ng per gallon, which is the detection limit of the assay (12), the milk gets diluted by a factor of ≈20 during processing, and hence each person consumes ≈4 ng in their quart of milk, which is 2 logs less than the estimated ID_{50} for children, using the human data. Therefore, the current test can afford to lose some of this sensitivity if it leads to increased specificity or speed. An alternative less-sensitive ELISA assay based on the catalytic activity of the toxin is also available for botulinum toxin A (21) [List Biological Laboratories (Campbell, CA), www.listlabs.com, accessed on July 1, 2004] and may be more specific in foods (unlike milk) where the toxin is unstable.

Current antibiotic residue testing takes 45 min, during which time the truck waits before having its contents drained into a silo.

Table 3. Sensitivity analysis for five parameters in the no-detection case

Case description	Release size 0.1 g	1 g	10 g	100 g	1 kg
Base case	2.3×10^3	1.5×10^5	5.0×10^5	5.7×10^5	5.7×10^5
Time between silo cleanings = 48 hr	2.8×10^3	1.6×10^5	3.8×10^5	3.9×10^5	3.9×10^5
Silo size = 100,000 gallons	2.1×10^2	1.4×10^5	8.4×10^5	1.1×10^6	1.1×10^6
Silos per processing line = 4	4.4×10^1	1.1×10^5	1.2×10^6	2.2×10^6	2.2×10^6
Inactivation by pasteurization = 0.99	6.6×10^{-11}	5.0	3.8×10^4	3.6×10^5	5.7×10^5
ID_{50} (adult, child) = 70 μg, 30 μg	1.8×10^{-16}	6.7×10^{-3}	7.5×10^3	2.1×10^5	5.3×10^5

Each change from the base-case value in Table 1 was made in isolation, and the mean number of poisoned people was computed for four different release sizes.

A test that takes >45 min is impractical because it either would increase the waiting time for each truck (if milk is not released to the silo until the test results are received) or would need to have near-perfect specificity (if milk is released before the test results are received). In contrast, three possible approaches can be used to deal with a positive result from a sub-45-min test: the truck can be held until a confirmatory mouse assay is performed, the milk can be discarded, or the milk can be routed to a processing line for ultra-high-temperature pasteurization, which kills all of the botulinum toxin. The likelihood that positively tested milk contains toxin may be extremely small, e.g., by Bayes' rule, if there is a 10% probability of an attack occurring in the U.S. over the next 5 years, and the false-positive rate is 10^{-4}, then the probability that positively tested milk contains toxin is only 5×10^{-5}. Regardless of which of the three options is used, it seems clear that a sub-45-min test is necessary from a practical perspective. Even if such a test is not perfectly specific, it could still be an immensely useful tool that could essentially eliminate the threat of this scenario. Even if the total cost of a test was $50, testing each 5,500-gallon truck would increase the cost of milk by only 1 cent per gallon. In addition, because thousands of people would be poisoned per hour in this scenario, it is imperative to perfect the design and implementation of a near-instantaneous product recall and disposal strategy.

To understand the impact of changing these processing parameters and to assess the danger of bioterror threats to various food industries, we need some understanding of the terrorists' capabilities. To put the release sizes in Figs. 2 and 3 into perspective, we note that the maximum concentration of botulinum toxin in culture is $2–3 \times 10^6$ mouse units per ml (22), where a mouse unit is the mouse intraperitoneal LD_{50} in micrograms. In the 1980s, the Iraqi bioweapons program apparently increased this concentration 5- to 10-fold with the use of sulfuric acid (23). If so, it would appear that terrorists should be capable of a concentration of at least 3×10^7 mouse units per ml = 4 g per gallon. That is, a terrorist with this technology could easily deliver 10 g of toxin without any special gear. Referring to Fig. 2, in the absence of detection, this amount would poison >400,000 people. Delivering 100 g or more with this technology would be more cumbersome and would greatly increase the likelihood of intercepting the attack. Amplification technologies have advanced significantly in recent years (24), and hence terrorists may be capable of concentrations considerably higher than 4 g per gallon.

Section 5 of *Supporting Appendix* analyzes three additional interrelated issues: secondary cases due to crosscontaminated milk, product tracing, and product recall. Two locations in the supply chain, trucks that are cleaned daily but that make two trips daily and processing lines that are cleaned daily, offer the opportunity for uncontaminated milk to become tainted by uncleaned residue from the primary release. The secondary effect from a release in a truck has an ≈50% chance of causing damage equivalent to a release that is 8 h later and ≈0.5% as large as the primary release. According to Figs. 2 and 3, secondary casualties would be significant only in cases when the primary release poisons nearly all of its consumers (in the absence of detection). The secondary impact due to tainted processing lines is likely to be much smaller, but the resulting milk concentrations are more difficult to estimate.

This potential for crosscontamination, coupled with consumer anxiety, would probably cause the supply chain's entire milk supply to be recalled and discarded at the time of detection. For the values in Tables 4 and 5, which are published as supporting information on the PNAS web site, this amounts to 4.83 million gallons, which includes 2.24-million-gallon containers of partially consumed milk that need to be recalled from consumers (Eq. **29** in *Supporting Appendix*). In addition, 640,000 gallons per day of freshly produced milk would need to be discarded until the attack is effectively investigated, the supply chain is turned back on, and consumer confidence returns. This delay could be hastened by effective product tracing, decontamination, and risk communication. The U.S. dairy industry traces every milk carton back to its processing facility, which, at least in theory, prevents the entire nation's milk supply (≈300 million gallons) from being discarded and recalled. In other food scenarios where there is no risk of crosscontamination (e.g., fresh produce packaged in the field), the ability to trace a product back through the particular path it takes in Fig. 1 could lead to a significant reduction in the amount of product recalled and discarded. As an illustration, we compute (Eq. **30** in *Supporting Appendix* and Table 6, which is published as supporting information on the PNAS web site) the amount of milk that needs to be discarded as a function of the release location (farm, truck, or silo) and the stage (cow, farm, truck, silo, or processing facility) to which the milk can be traced, hypothetically assuming no crosscontamination.

Our sensitivity analysis suggests there are three types of variables. Variables of the first type (time between silo cleanings, silo size, and number of silos per processing line) cause a vertical shift in the number poisoned vs. release size graphs (Fig. 5 *a–c*, which is published as supporting information on the PNAS web site) and underscore the subtle relationship between high production efficiency and the consequences of a bioterror attack. Economies of scale can represent a double-edged sword: increasing the time between silo cleanings, silo size, or number of silos per processing line increases the amount of contaminated milk but reduces the toxin concentration of this milk, thereby mitigating the impact of a small release and exacerbating the effect of a large release. However, for the parameter regimes considered here, the reduction in casualties in a small release is very modest, whereas the increase in casualties in a large release with no testing and poor detection is in the hundreds of thousands. Variables of the second type (ID_{50}, pasteurization inactivation) result in a horizontal shift in the number poisoned vs. release size graphs (Fig. 5 *d* and *g*). More precisely, to cause equivalent damage, the release size for the monkey ID_{50}s needs to be 70 times larger than the release size for the human ID_{50}s. Similarly, to generate an equivalent casualty level, the release size in the 99% inactivation scenario needs to be 1–0.684/1–0.99 = 31.6 times larger than the release size in the 68.4% inactivation scenario. Variables of the third type (distribution speed, consumption rate, children's incubation, number of symptomatics until detection, and milkborne detection time) all relate to the speed of various events and have no impact on the casualty level if the attack is not detected. In the no-testing case, the resulting graphs (Fig. 5 *e–f* and *h–j*) are very similar to one another and, for the parameter values considered here, the change in the children's incubation has the biggest impact, and the consumption rate has the smallest impact.

Conclusion

In closing, it is important to stress that several elements of the model contain enough irreducible uncertainty to preclude estimating the impact of an attack to within several orders of magnitude. First and foremost is the dose–response curve. The paucity of human data makes an estimate of the ID_{50} a difficult task, and a reliable estimate of the probit slope is impossible. The ID_{50} values used here are not close to the worst-case estimate, due to the possibility that several sublethal (injected or oral) doses collectively containing 1–10% of the LD_{50} may be lethal, as in guinea pigs, rabbits, and mice (25). There are also three aspects of the model that have not been discussed in the open literature, although presumably studies can and perhaps have been performed: the inactivation rate attained by pasteurization, the specificity of an ELISA test in milk, and the release size that a terrorist organization is capable of. Such studies would allow our results to be sharpened considerably. The dose–response curve, pasteurization inactivation rate, and terrorists' release-size capabilities each contain several orders of magnitude of uncertainty, and together they essentially determine the release threshold required to achieve a sufficiently high milk concentration. There is much less uncertainty about how many people would drink this contaminated milk. There is irreducible uncertainty due to the timing of the release within the silo operation cycle, which causes the number poisoned to be roughly uniformly distributed between half and twice the mean values (with an additional point mass at the latter value with probability 0.26) reported in Figs. 2 and 3.

Taken together, we have a reasonably accurate estimate of the number of people who could be poisoned but a very poor estimate of how much toxin is required to cause a large outbreak. The main uncertainties related to the number of people who could be poisoned are how quickly the attack would be detected via early symptomatics and how quickly and completely consumption would be halted: we optimistically assumed that consumption is halted instantaneously and completely within 24 h after the early symptomatics are detected, even though it took several weeks to identify the source of the two large but more subtle *Salmonella* outbreaks in the dairy industry (26, 27). Even if the reducible uncertainty resolves itself favorably (e.g., heat pasteurization inactivates 99% of toxin rather than 68.4%), a catastrophic event is not implausible, and the way forward seems clear: invest in prevention, investigate inactivation processes that do not affect nutrition or taste and, most importantly, develop and deploy a sub-45-min highly specific in-process test.

Although the U.S. government appears to be working diligently on the latter two issues, it is not clear how quickly and thoroughly the dairy supply chain is being secured. The use of voluntary Food and Drug Administration guidelines is not commensurate with the severity of this threat, and the government needs to act much more decisively to safeguard its citizens from such an attack. Moreover, although the dairy industry is an obvious target, the government needs to force other food processing industries to quickly assess the impact of a deliberate botulinum release in their supply chains and to do what is necessary to prevent and mitigate such an event.

L.M.W. thanks Stephen Arnon, Larry Barrett, Seth Carus, Richard Danzig, Clay Detlefson, Leland Ellis, Jerry Gillespie, Steve Jerkins, Eric Johnson, Laura Kelley, David Montague, Keith Ward, and Dennis Wilson for helpful conversations. This research was partially supported by the Center for Social Innovation, Graduate School of Business, Stanford University.

1. Danzig, R. (2003) *Catastrophic Bioterrorism–What is to be Done?* (Center for Technology and National Security Policy, National Defense University, Washington, DC).
2. Kaplan, E. H., Craft, D. L. & Wein, L. M. (2002) *Proc. Natl. Acad. Sci. USA* **99**, 10934–10940.
3. Halloran, M., Longini, I. M., Jr., Nizam, A. & Yang, Y. (2002) *Science* **298**, 1428–1433.
4. Eubank, S., Guclu, H., Kumar, V. S. A., Marathe, M. V., Srinivasan, A., Toroczkai, Z. & Wang, N. (2004) *Nature* **429**, 180–184.
5. Wein, L. M., Craft, D. L. & Kaplan, E. H. (2003) *Proc. Natl. Acad. Sci. USA* **100**, 4346–4351.
6. Sobel, J., Khan, A. S. & Swerdlow, D. L. (2002) *Lancet* **359**, 874–880.
7. Woodburn, M. J., Somers, E., Rodriguez, J. & Schantz, E. J. (1979) *J. Food Sci.* **44**, 1658–1661.
8. Meyer, K. F. & Eddie, B. (1951) *Zeitschr. Hyg.* **133**, 255–263.
9. Morton, H. E. (1961) *The Toxicity of Clostridium botulinum Type A Toxin for Various Species of Animals* (Institute of Cooperative Research, University of Pennsylvania, Philadelphia).
10. Terranova, W., Breman, J. G., Locey, R. P. & Speck, S. (1978) *Am. J. Epidemiol.* **108**, 150–156.
11. Schantz, E. J. & Sugiyama, H. (1974) *J. Agr. Food Chem.* **22**, 26–30.
12. Ferreira, J. L., Maslanka, S., Johnson, E. & Goodnough, M. (2003) *J. AOAC Int.* **86**, 314–331.
13. Herrero, B. A., Ecklund, A. E., Streett, C. S., Ford, D. F. & King, J. K. (1967) *Exp. Mol. Pathol.* **6**, 84–95.
14. Shapiro, R. L., Hatheway, C., Becher, J. & Swerdlow, D. L. (1997) *J. Am. Med. Assoc.* **278**, 433–435.
15. Reed, B. A. & Grivetti, L. E. (2000) *J. Dairy Sci.* **83**, 2988–2991.
16. U.S. Food and Drug Administration (2003) *Dairy Farms, Bulk Milk Transporters, Bulk Milk Transfer Stations and Fluid Milk Processors: Food Security Preventive Measures Guidance* (U.S. Food and Drug Admin., Washington, DC).
17. Siegel, L. S. (1993) in *Clostridium botulinum: Ecology and Control in Foods*, eds. Hauschild, A. H. W. & Dodds, K. L. (Dekker, New York), pp. 323–341.
18. U.S. Department of Defense (1996) *Army Field Manual 8-9*, Navy Medical Publication 5059 and Air Force Joint Manual 44-151 (U.S. Department of Defense, Washington, DC).
19. Arnon, S. S., Schechter, R., Inglesby, T. V., Henderson, D. A., Bartlett, J. G., Ascher, M. S., Eitzen, E., Fine, A. D., Hauer, J., Layton, M., *et al.* (2001) *J. Am. Med. Assoc.* **285**, 1059–1070.
20. St. John, R., Finlay, B. & Blair, C. (2001) *Can. J. Infect. Dis.* **12**, 275–284.
21. Wictome, M., Newton, K. A., Jameson, K., Dunnigan, P., Clarke, S., Gaze, J., Tauk, A., Foster, K. A. & Shone, C. C. (1999) *FEMS Immunol. Med. Microbiol.* **24**, 319–323.
22. Dasgupta, B. R. (1971) *J. Bacteriol.* **108**, 1051–1057.
23. Miller, J. (April 27, 2003) *N.Y. Times*, p. 22.
24. Danzig, R. (2005) in *The Challenge of Proliferation: A Report of the Aspen Strategy Group*, ed. Campbell, K. (The Aspen Institute, Washington, DC), in press.
25. Matveev, K. I. (1959) *J. Microbiol. Epidemiol. Immunobiol.* **30**, 71–78.
26. Ryan, C. A., Nickels, M. K., Hargrett-Bean, N. T., Potter, M. E., Endo, T., Mayer, L., Langkop, C. W., Gibson, C., MacDonald, R. C., Kenney, R. T., *et al.* (1987) *J. Am. Med. Assoc.* **258**, 3269–3274.
27. Hennessy, T. W., Hedberg, C. W., Slutsker, L., White, K. E., Besser-Wiek, J. M., Moen, M. E., Feldman, J., Coleman, W. W., Edmonson, L. M., MacDonald, K. L., *et al.* (1996) *New Engl. J. Med.* **334**, 1281–1286.

総合科学技術会議
安全に資する科学技術推進プロジェクトチーム
第4回会合用資料

資料4－2

内閣官房における安全に資する科学技術の推進について

平成17年3月4日（金）
内閣官房副長官補（安全保障・危機管理担当）付

目次

1　内閣官房の役割

○　内閣官房の役割

内　閣（内閣総理大臣）

内閣官房が政府としての危機管理を担当

内　閣　官　房（内閣官房長官）

各省庁の総合調整

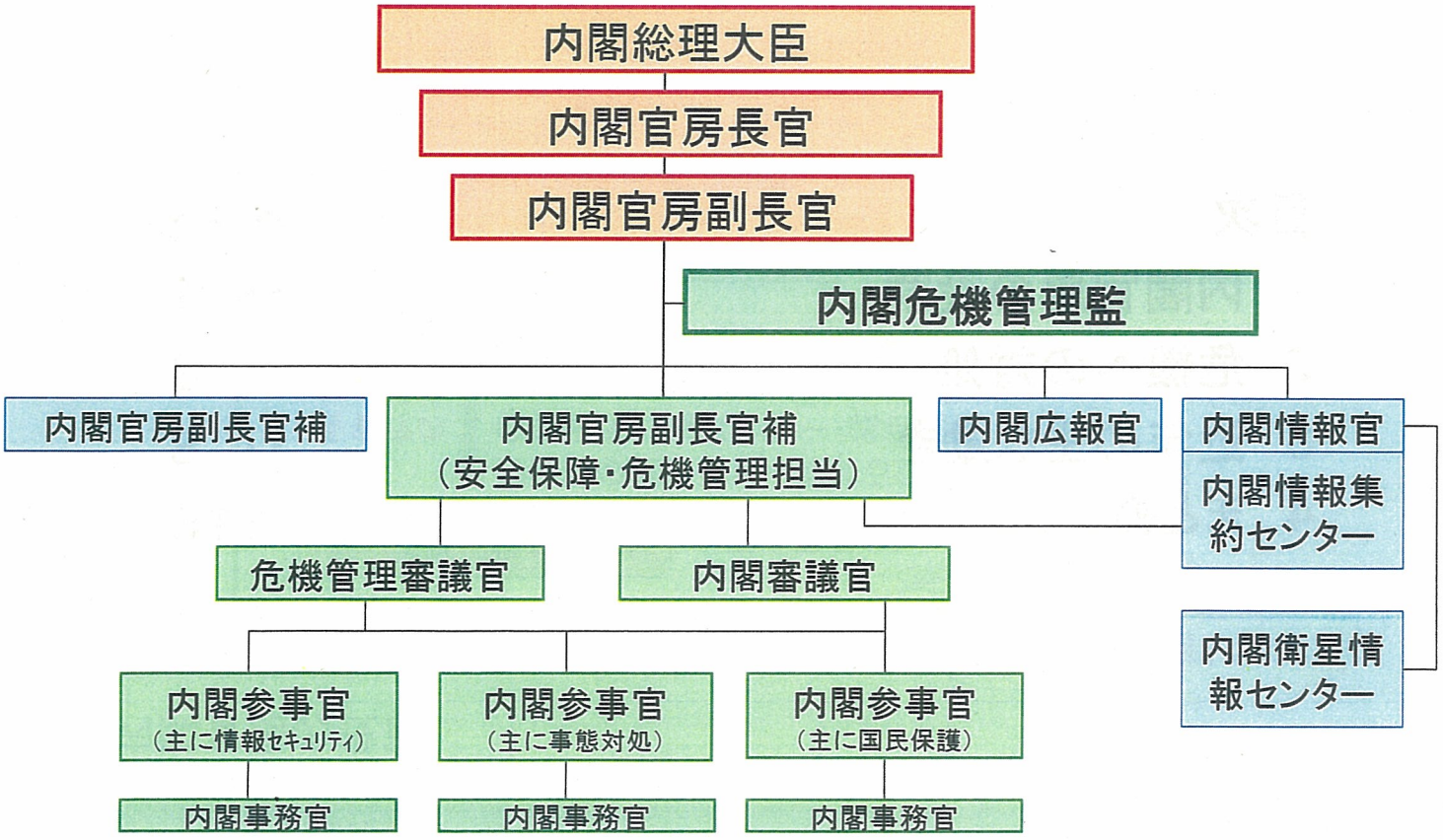
- ○内閣の重要政策に関する企画・立案・総合調整
- ○各省庁の施策の統一・総合調整
- ○内閣官房の調整は最高かつ最終
- ○危機管理は内閣の重要政策

内閣府（科学技術、防災などの施策の総合調整/内閣官房を助ける）

各省庁：所掌に応じ施策を実施

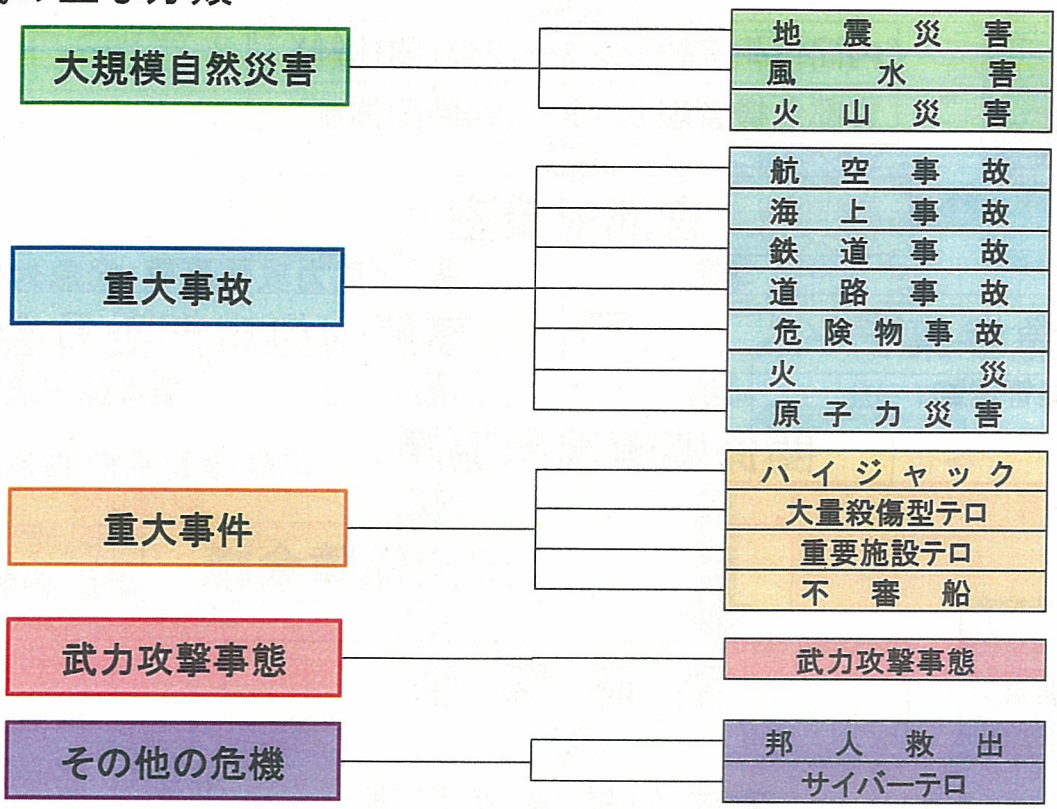
・警察庁　・防衛庁　・総務省　・国土交通省　・法務省
・外務省　・財務省　・文部科学省　・厚生労働省
・農林水産省　・経済産業省　・環境省　等

○内閣官房の危機管理に関する組織

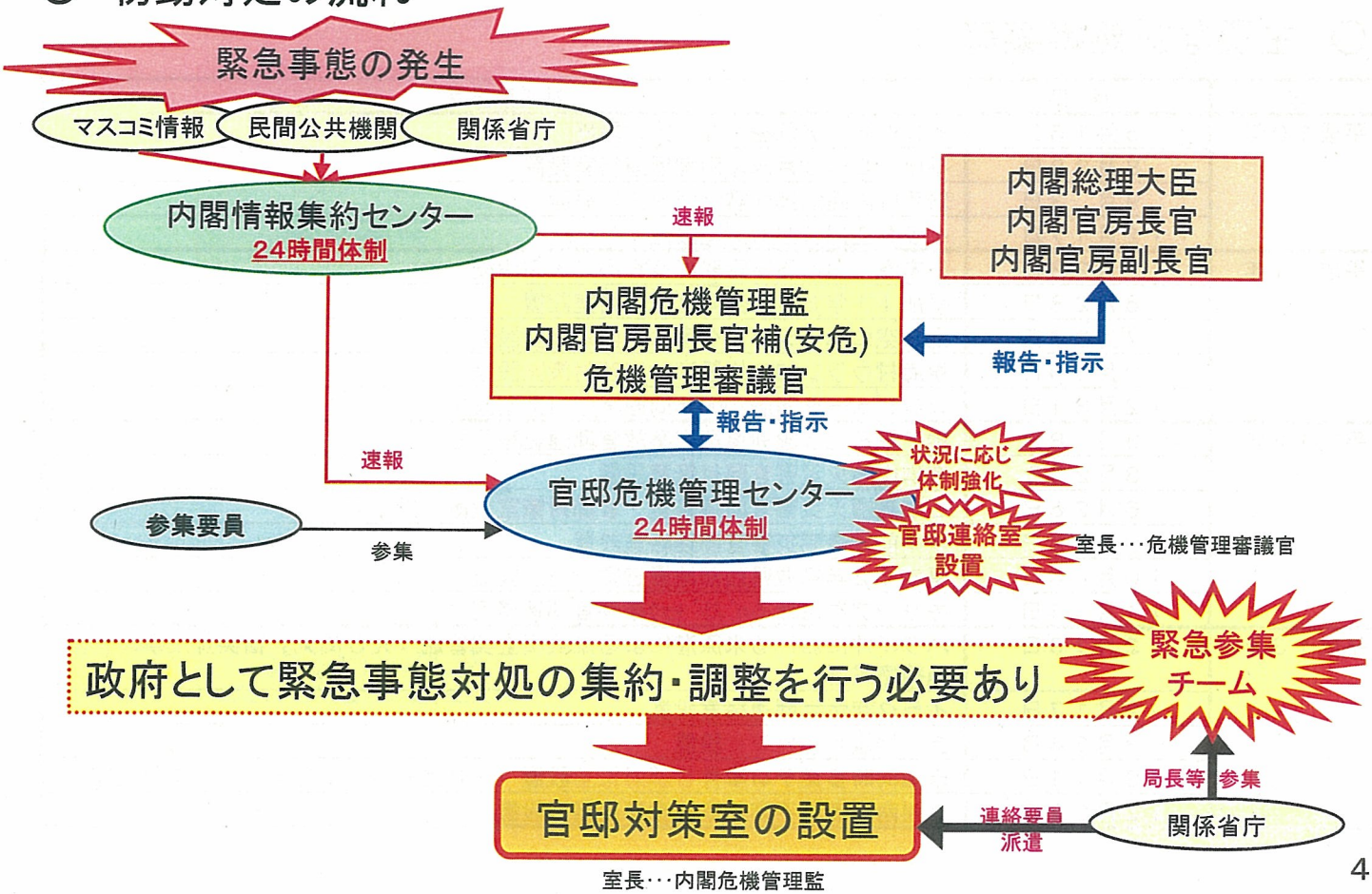


2 危機への対処

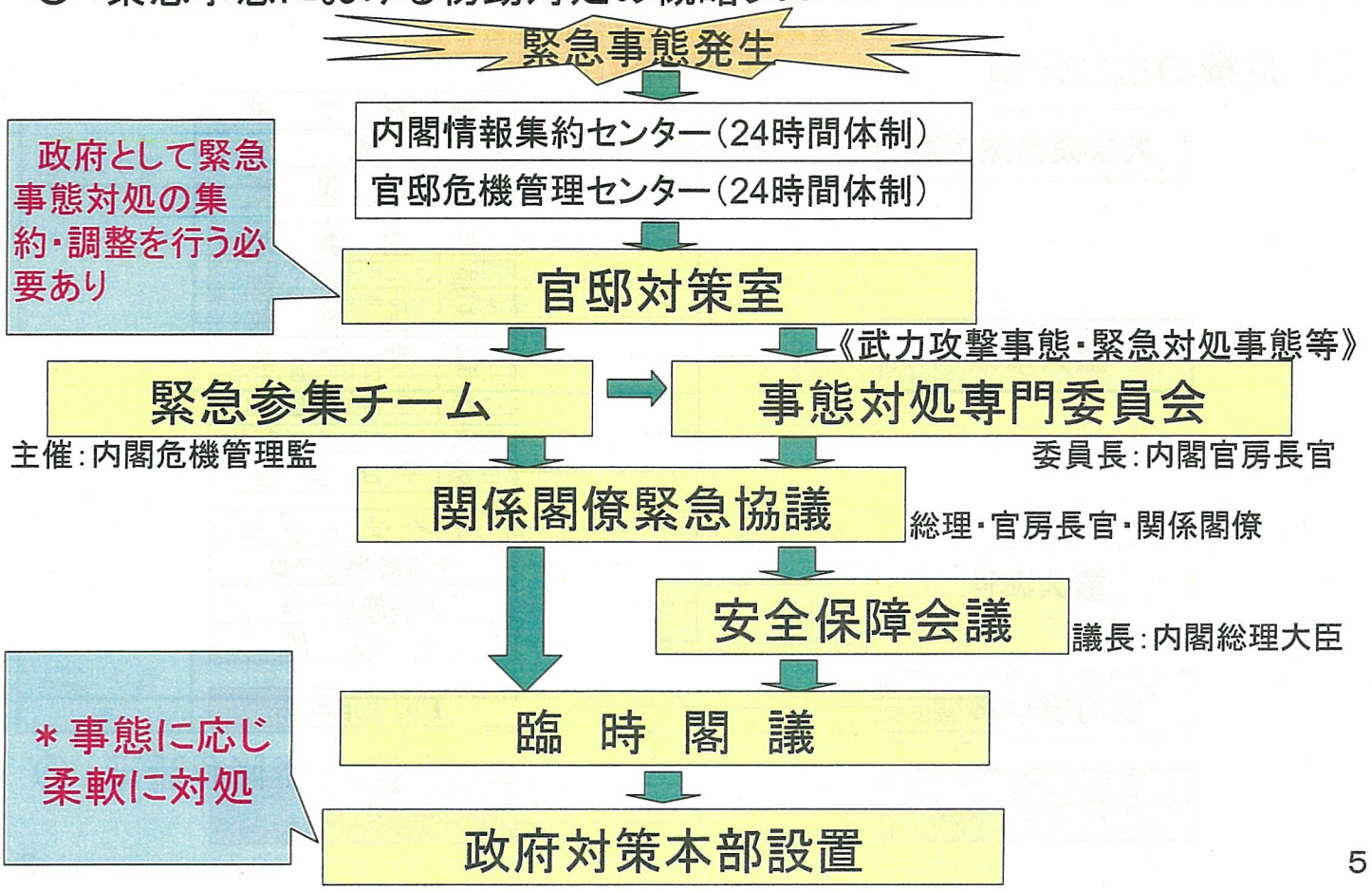
○ 危機の主な分類



○ 初動対処の流れ



○ 緊急事態における初動対処の概略フロー



○ 主要な対処事案等①

年	月　日	対処事案等
平成１０年	５月１５日	インドネシア危機官邸対策室設置
	８月２８日	平成１０年８月末豪雨官邸連絡室設置
	９月　３日	岩手県内陸北部地震官邸対策室設置
	１２月１７日	イラク空爆官邸対策室設置
平成１１年	３月２３日	日本海における不審船事案官邸対策室設置
	６月２８日	平成１１年６月末豪雨官邸連絡室設置
	７月２３日	全日空機ハイジャック事件官邸対策室設置
	９月３０日	東海村ウラン加工施設事故官邸対策室設置
	１２月３１日	コンピュータ西暦2000年問題官邸対策室設置
平成１２年	３月　８日	地下鉄日比谷線列車衝突事故官邸連絡室設置
	３月２９日	有珠山噴火災害官邸対策室設置
	６月２６日～	三宅島噴火災害官邸連絡室・官邸対策室設置（計６回）
	９月１２日	秋雨前線豪雨災害官邸連絡室設置
	１０月　６日	平成１２年鳥取県西部地震官邸対策室設置
	１１月　４日	ギリシアにおけるﾊﾞｽｼﾞｬｯｸ事件官邸連絡室
平成１３年	２月１０日	ハワイ沖における米原潜による漁業調査実習船「えひめ丸」衝突沈没事故官邸連絡室設置
	２月１７日	イラク空爆官邸連絡室設置
	３月２４日	芸予地震官邸対策室設置
	９月１１日	米国同時多発テロ事件官邸対策室設置（１０月８日に緊急テロ対策本部設置）
	１２月２２日	九州南西海域不審船事案官邸連絡室設置

○ 主要な対処事案等②

年	月 日	対処事案等
平成１４年	３月２６日	石垣島南方沖を震源とする地震による津波対応官邸連絡室設置
	３月３１日	台湾付近を震源とする地震による津波対応官邸連絡室設置
平成１５年	（３月２０日）	（イラク問題対策本部設置）
	５月２６日	宮城県沖地震官邸対策室設置
	７月２６日	宮城県北部地震官邸対策室設置
	９月２６日	十勝沖地震官邸対策室設置
平成１６年	４月　８日	在イラク邦人人質事件官邸対策室設置（４月９日に在イラク邦人人質事件対策本部設置
	５月２８日	在イラク邦人襲撃被害事件官邸対策室設置
	８月　９日	関西電力美浜原子力発電所３号機タービン建屋内蒸気漏れ事故に関する連絡室設置
	８月２５日	ロシア機墜落に係る連絡室設置
	９月　６日	東海道沖を震源とする地震による津波に関する連絡室設置
	９月２３日	北朝鮮の弾道ミサイルに関連する連絡室設置
	１０月２１日	台風２３号被害に関する官邸連絡室設置
	１０月２３日	新潟県中越地震官邸対策室設置
	１０月２７日	在イラク邦人人質事件官邸対策室設置
	１１月１０日	先島諸島周辺海域潜水航行事案官邸対策室設置
	１１月２９日	釧路沖を震源とする地震に関する官邸連絡室設置
	１２月　６日	根室半島南東沖を震源とする地震に関する官邸連絡室設置
	１２月１４日	留萌市庁南部を震源とする地震に関する官邸連絡室設置
	１２月２７日	インドネシア・アチェ特別州沖の大規模地震に関する官邸連絡室設置

3　近年の主な動き

○内閣を中心とする緊急事態対処体制整備の主な経緯

平成　7年　2月	大規模災害に対応する緊急参集チームを設置 情報伝達窓口を内閣情報調査室とする閣議決定
平成　8年　4月	官邸に危機管理センターを設置
平成　8年　5月	官邸に24時間体制の内閣情報集約センターを設置
（平成9年　5月）	（内閣の危機管理機能の強化に関する行政改革会議の意見集約）
平成10年　4月	内閣危機管理監を設置 内閣安全保障室を内閣安全保障・危機管理室に改組
平成10年　4月	重大テロ発生時の政府の初動措置を閣議決定
平成13年11月	不審船への政府の初動措置を閣議決定
平成14年　4月	新官邸危機管理センターの運用開始
平成15年　6月	安全保障会議の下に事態対処専門委員会を設置
平成15年11月	あらゆる緊急事態への政府の初動対処体制について閣議決定 各種事案に対応する緊急参集チームを新たに構成

3 近年の主な動き

○ 安心・安全な国家を形成するための総合的な取り組み

① 法制度等の確立

1）安全保障・防衛力の見直し

・安全保障と防衛力に関する懇談会、防衛計画の大綱（平成16年12月閣議決定） 等

2）有事関連法案の成立、施行

・事態対処法（平成15年6月）、国民保護法（平成16年9月） 等

3）国際テロ対策

・空港・港湾における水際対策・危機管理体制の強化（平成16年1月）
・テロの未然防止に関する行動計画の策定（平成16年12月） 等

② 体制の改善

1）緊急事態対処の明確化（平成15年11月閣議決定）

・様々な緊急事態に総合的に対処できるよう、すべての緊急事態における政府としての初動対処体制について明確化

2）危機管理関係省庁連絡会議の開催

3）情報収集衛星の運用開始

・内閣衛星情報センターの設置（平成13年4月）、情報収集衛星打ち上げ（平成15年3月）、本格運用開始（平成16年4月～）

4）その他

・内閣官房沖縄危機管理監の設置（平成16年10月）

有事関連法案の成立、施行

武 力 攻 撃 事 態 対 処 法

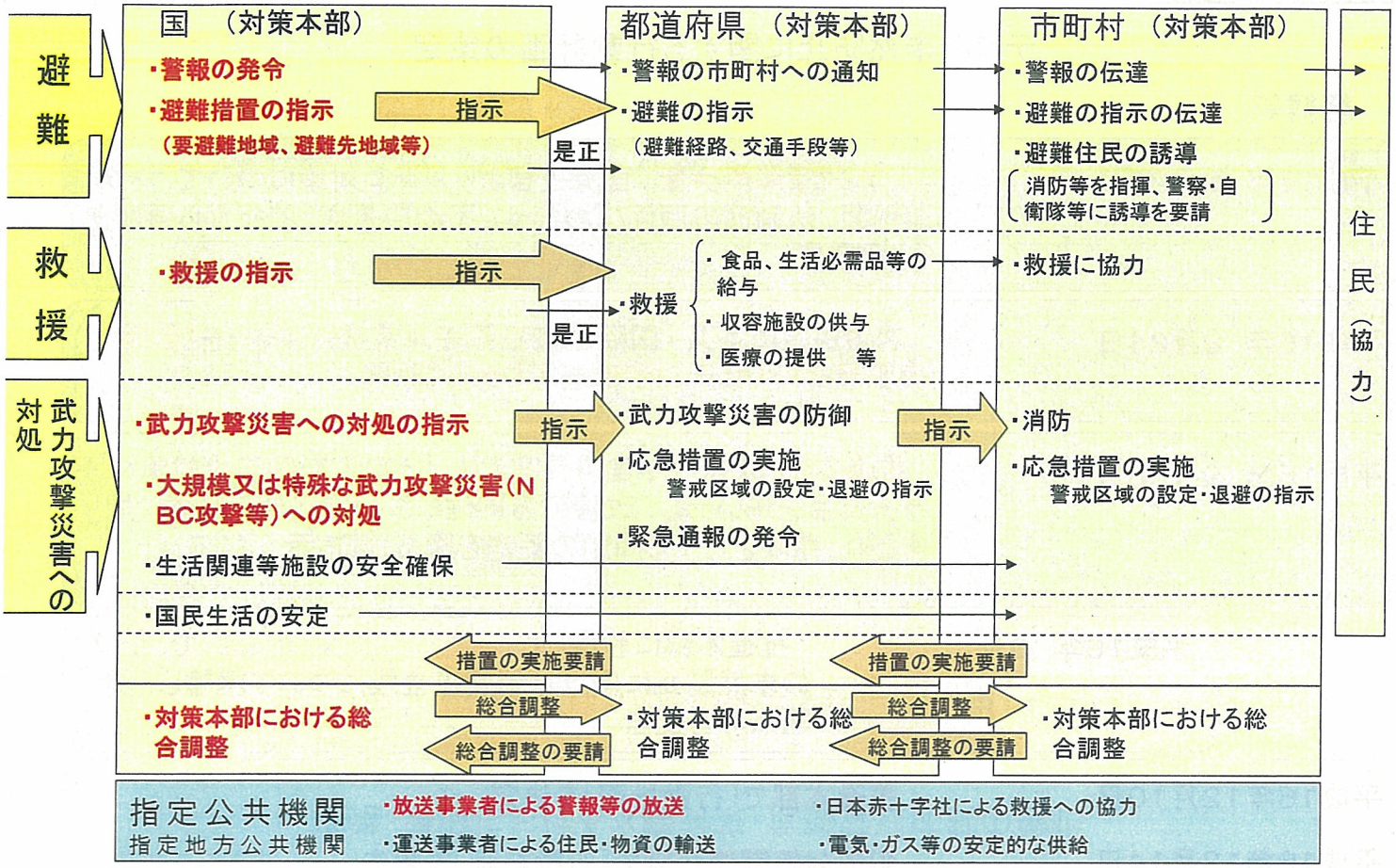
○ 武力攻撃事態等への対処について、基本理念、国・地方公共団体等の責務、対処基本方針の内容、決定手続等基本的事項を定めるもの

武力攻撃事態対処法に定められた整備すべき個別の法制

- 国民保護法
- 米軍行動関連措置法
- 海上輸送規制法
- 自衛隊法の一部改正
- 特定公共施設利用法
- 国際人道法違反処罰法
- 捕虜取扱い法

武力攻撃から国民の生命・身体及び財産を保護し、国民生活等に及ぼす影響を最小にするため、国・地方公共団体等の責務、避難・救援・武力攻撃災害への対処等の措置を規定

国民の保護に関する措置の仕組み



国際テロ対策

空港・港湾における水際対策・危機管理体制の強化