



United States
Department of
Agriculture

Food Safety
and Inspection
Service

Washington, D.C.
20250

OCT 7 2011

Ms. Rosemary Mucklow
Director Emeritus
National Meat Association
1970 Broadway, Suite 825
Oakland, California 94612

Dear Ms. Mucklow:

Thank you for your letter of August 8, 2011, inquiring about the protocols that the Food Safety and Inspection Service (FSIS) is applying to protect establishment proprietary and confidential information as the Agency implements the Public Health Information System (PHIS). I was very pleased to speak to the National Meat Association's (NMA) Summer Conference in Utah and enjoyed our discussions.

I assure you that FSIS takes full responsibility for the security of confidential plant information in Agency systems, and afforded to Agency employees for conducting inspection and investigation activities. I want to thoroughly explain the protective measures used by FSIS as it strives to protect the public health while meeting its responsibility to ensure the security of proprietary and confidential information in all inspected establishments.

All FSIS employees take an oath upon entering the service to faithfully discharge the duties of the office they are entering. This marks the beginning of employee responsibilities and is the foundation for FSIS' protective measures, which include the following:

1. Federal laws and statutes, which target disclosure, misappropriation, or theft of trade secrets, including those below:

- The Trade Secret Act (18 U.S.C. 1905), which applies to disclosure by a Government employee of trade secret, confidential commercial, or financial information provided to the Government by a company or other nongovernment organization. The criminal penalty for violating this law is termination of employment, a fine of not more than \$1,000, and imprisonment for not more than 1 year.
- The Economic Espionage Act (18 U.S.C. 1831-39), which makes the misappropriation or theft of trade secrets by any person a crime.

- The Food, Conservation, and Energy Act of 2008 (7 U.S.C. 8791), which created new provisions to protect agricultural information from disclosure. The law covers confidentiality, safeguarding, and disclosure and release restrictions.
2. Agency policies that define the responsibility for maintaining and protecting the confidentiality of plant information, delineated in extracts from directives below:
- FSIS Directive 4735.6, which addresses safeguarding confidential industry information, notes that “It is FSIS policy to protect the confidentiality of certain industry information to which Agency personnel are afforded privileged access while carrying out their responsibilities. Such information should be presumed to be confidential. Under 18 U.S.C. 1905, dissemination of product formulations or other trade secrets may be a criminal offense.”
 - Directive 1400.1, which informs employees with access to Agency records of their responsibilities and of the limitations on the release of both Government and private sector information, states that, “Trade secrets and commercial or financial information are privileged or confidential information. Unlawful disclosure of commercial or financial information could cause competitive harm to the company that owns the information. The protection of this information is not discretionary and individuals can be held personally liable for unlawful release of such information. Examples include product formulations, Hazard Analysis and Critical Control Point plans, Sanitation Standard Operating Procedures, production data, line speeds, and financial information.”
3. Security requirements, uniformly met by FSIS information systems, defined in the following laws, regulations, and guidelines:
- USDA Departmental Regulation 3505-003 Access Control Policy
 - Public Law 107-347, 44 U.S.C. 3531 et seq. E-Government Act of December 2002, Title III, Federal Information Security Management Act
 - Office of Management and Budget Memorandum 04-04, E-Authentication
 - National Institute of Standards and Technology Federal Information Processing Standards

These security requirements strictly define access and control of information. For PHIS, this means that only individuals authorized by USDA will have access to the records in this system. Role-based access controls are used, and access to the system itself is through use of an encrypted password, managed through the USDA’s e-Authentication system. User roles are restrictive and allow a minimal level of access to permit the adequate performance of job functions. Users are granted system access only upon successful completion of security training and must successfully complete security training each year to retain access. In addition, secure passwords are required to be changed frequently.

Ms. Rosemary Mucklow
Page 3

I hope that this information reassures NMA and its membership. I look forward to working with you and your members to implement PHIS, and to meet our mutual public health goals.

Sincerely,

A handwritten signature in black ink, appearing to read "Alfred V. Almanza". The signature is fluid and cursive, with a large, sweeping flourish at the end.

Alfred V. Almanza
Administrator