

# ACTION PLAN

**Issue Group:** Information Technology

**Specific Activity Area being Addressed by this Action Plan:** Confidentiality

## **Safeguarding Review Recommendations Covered:**

There were few recommendations that specifically mentioned confidentiality, however, it is clear that to carry out the recommendations regarding laboratory networks and surveillance, confidentiality concerns will need to be addressed.

#5 - Secure the appropriate authority for access to sampling and information needed to implement the NSS.

#130 - Incorporate the analysis of epidemiologic information and resource management. Make appropriate training available to state and federal animal health officials for the purpose of animal health emergency. Ensure that software and hardware resources meet program needs, and are compatible with those used by the states. Maintain confidentiality of sensitive information.

## **Issue Group Findings:**

In order to carry out its mission, VS collects and holds information about businesses and private citizens. A list of key VS information collection systems containing such information is provided in Attachment 1. Procedures for the collection, holding, and further disclosure of this information are governed by several laws including the: Privacy Act (PA), Freedom of Information Act (FOIA), Trade Secrets Act, and E-Government Act. Until passage of the Agricultural Bioterrorism Act of 2002, VS (unlike DHS, the Census Bureau, and the IRS, for example) did not have any specific statutes guiding its collection and disclosure of information. The Agricultural Bioterrorism Act contains a non-disclosure provision for certain types of information pertaining to select agents and toxins (see summary in Attachment 2).

The information environment is changing. Improved technology allows the linking of data collected in individual systems. GIS technologies allow the linkage of information about persons and business entities with “contextual” information via geospatial codes, i.e., demographic/environmental information. While linking this information has the potential to improve the efficiency of VS operations, quicken the speed of response to disease events, and allow increased understanding about disease dynamics, these linkages also heighten privacy/confidentiality concerns of the public (GAO, Record Linkage and Privacy). *“Widespread use of computerized recordkeeping and the growth in the use of the Internet to collect and share information have resulted in public concern about the privacy of personal information collected by the government. These concerns include those related to the government’s ability to ensure the accuracy and confidentiality of information about individuals and prevent misuse of personal information”* (GAO, Information Management: Selected agencies handling of personal information).

VS is also operating in a period where the need to partner with other entities, federal, state, and private, is increasing. Homeland security and emergency response concerns, in particular, are leading VS to extend its partnering beyond its traditional cooperative program partners. As stated in the report, *The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets*, “*Protecting America’s critical infrastructures and key assets calls for a transition to a new national cooperative paradigm.... Homeland security, particularly in the context of critical infrastructure and key asset protection, is a shared responsibility that cannot be accomplished by the federal government alone. It requires coordinated action on the part of federal, state, and local governments; the private sector; and concerned citizens across the country.*”

A number of new laws also affect VS’ collection and use of information. The E-government Act of 2002 contains a provision requiring agencies to conduct Privacy Impact Assessments before: 1) developing or procuring IT systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public or 2) conducting new electronic collections of information in identifiable form for 10 or more persons. PIAs are also required when a change to an IT system creates new privacy risks such as when an agency employs new relational database technologies to access multiple data stores.

This new environment leaves VS facing three major issues related to confidentiality: 1) instilling confidence in those who share data with the agency that the information shared will be kept confidential, 2) developing mechanisms for sharing critical information with an increasing array of partners/cooperators to improve the effectiveness of animal health programs while maintaining appropriate levels of confidentiality, and 3) ensuring that VS is in compliance with current statutes. Each of these issues is discussed below, difficulties (roadblocks) the agency faces in addressing these concerns are noted, and current/potential actions VS is taking/can take are identified.

#### Ability to instill confidence in data providers

As stated above, laws such as the PA, FOIA, Trade Secrets, and E-government, mandate the types of information VS must share with the public and how such disclosures are to be made (see summary of each law in Attachment 2). These laws offer few absolutes regarding how particular information will be treated. The PA establishes that information about individuals cannot be further disclosed without prior written consent of the individual but there are exceptions provided in the law. These PA provisions, however, do not apply to businesses.

The FOIA was enacted to establish a right of the public to access information about the activities of the federal government. Disclosure of information is required by FOIA except under nine specific exemptions. To apply one of these exemptions, the federal agency must make a case for withholding the information. Because nondisclosure decisions are subject to legal challenge, there is no certainty that an agency nondisclosure decision based on one of the FOIA exemptions will be upheld. The quality of the agency argument and the agency’s adherence to procedural requirements set forth in the Act, can sometimes be a factor and, if found lacking, can result in information being disclosed that would otherwise have been exempted. Judges will also balance

public interest/benefit with the harm caused by disclosure and, in matters of public health, could favor disclosure.

Any collection of information maintained by an agency is considered a “record” and subject to FOIA disclosure rules. Paying a third party to hold information for an agency does not alter the information’s status as an agency record. Information obtained by other entities as part of cooperative agreements funded by the agency is also subject to the same FOIA disclosure requirements as information obtained directly by the federal government. The disclosure status of information held in databases shared by or with other parties is more complicated and the level of “control” the agency has over the information becomes a factor in applying FOIA disclosure rules. Under the FOIA, “control” is not determined solely based on possession; rather, it is a question of whether, after considering all of the circumstances, the records at issue are subject to free disposition. If the agency receives information from another source (i.e., private individual, business, contractor) that limits or greatly restricts the agency’s use, transfer, and disposition abilities, then it will not likely be deemed that the agency is in “control” of the information. For example, if in a shared database, the agency’s ability to access certain fields, change or input information, or maintain technical aspects of the system is limited, then the agency would have a strong argument for saying it does not own/control the information and thus should not be subject to determining its release. However, information input by the agency into such a database would be considered an agency record and subject to disclosure under the FOIA. If an outside entity provides the agency with a database for the agency to use in order to conduct an analysis but also provides clear instruction to the agency that the agency must return or destroy the data upon completion of the analysis, then the data would not likely be deemed to be in the agency’s control.

Current/potential actions VS is taking/can take:

- 1) **Minimize the amount of information that VS holds.** VS could review each of its data collection systems to ensure that only necessary information is collected and held. VS could also rely on states holding more information in separate databases. Relying on separate individual state systems could, however, decrease efficiency of operations and would not be possible for information which is a federal responsibility such as information on interstate and international movements of animals and animal products. State governments are also bound by their own freedom of information laws and some of these laws require more public disclosure of information than the federal government.
- 2) **Strengthen APHIS’ ability to make sound arguments for FOIA exemptions.** Take steps to ensure that information is submitted to the agency in a manner that improves the ability of the agency to argue for nondisclosure. For example, information which is provided voluntarily should be clearly marked as such when it is submitted to the agency. Such marking will help the agency in making a case for nondisclosure. (Note: voluntary submission alone does not secure the information from disclosure. In addition to being voluntarily provided to the government, submitters must show that the information falls within Exemption 4 (trade secrets, commercial and/or financial information) and is not information of a type that would customarily be released to the public by the submitter. The submitter has the burden to establish the likelihood of substantial competitive injury, and not merely the possibility of injury. As established through legal precedent, courts

have routinely upheld agency release determinations after first considering whether the information was voluntarily submitted and second, whether the information meets the criteria in FOIA to be considered confidential information.)

- 3) **Obtain designation of part of the agency as a statistical agency in order to protect the confidentiality of information collected for purely statistical purposes.** The Confidentiality Information Protection and Statistical Efficiency Act of 2002 (CIPSEA) (Title V of the E –Government Act) and the 1997 OMB Order Providing for the Confidentiality of Statistical Information afford a confidential status to some information collected by designated statistical agencies (see additional description in Attachment 2). Information collected for statistical purposes, i.e., information which is collected to describe, estimate, or analyze characteristics of groups without identifying the individual or organizations that comprise such groups, must be held confidential under the Act. The CIPSEA ensures that information supplied by individuals or organizations to an agency for statistical purposes under a pledge of confidentiality is used exclusively for statistical purposes and that such information will not be disclosed in identifiable form to anyone not authorized. The CIPSEA also requires statistical agencies to clearly distinguish any data or information it collects for nonstatistical purposes and to inform the public prior to the collection of such information. Obtaining statistical agency status for VS or part of VS (such as CEAH) would allow VS to improve the confidentiality protections under both the PA and FOIA for NAHMS study data as well as other baseline data or statistical information. Confidential status under the CIPSEA does not extend to other VS surveillance and disease eradication data as that data is not used for statistical purposes, rather decisions are made and actions are taken regarding individual operations based on the information.
- 4) **Seek legislation which creates specific confidentiality and disclosure requirements for information collected by VS.** A number of agencies have separate statutes guiding the disclosure of information collected by those agencies. FOIA Exemption 3 applies to matters “specifically exempted from disclosure by [a] statute” other than FOIA. To support an Exemption 3 claim, an agency must invoke a statute which prohibits/protects the information from disclosure. The Census Bureau and IRS have long standing statutes that they can invoke in supporting an Exemption 3 claim. The Homeland Security Act of 2002 which created the Department of Homeland Security (see summary in Attachment 3) included provisions regarding the disclosure of critical infrastructure information obtained by the Department which allows DHS to support an Exemption 3 claim for this type of information. The Transportation Security Administration also has a separate statute that it can invoke to support an Exemption 3 claim for certain types of information which it collects. Both the DHS and TSA exemptions are limited to very specific types of data. In the interim rule issued by DHS setting forth its procedures for handling critical infrastructure information, DHS further refined and limited the critical infrastructure information to which the FOIA exemption would apply. The Agricultural Bioterrorism Act of 2002 provided APHIS with the ability to invoke an Exemption 3 claim for nondisclosure of some information concerning select agents. APHIS may be given additional nondisclosure provisions in a Congressionally mandated animal identification system. Several bills introduced recently in Congress which call for the establishment of a nationwide livestock identification system contain language which would exempt information collected under the animal ID system from FOIA (H.R. 3787,

National Farm Animal Identification and Records Act and S. 2070 US Animal Identification Plan Implementation Act). Passage of one of these bills would provide the APHIS Freedom of Information staff with the authority to withhold specific information associated with the livestock identification system. APHIS is also exploring crafting legislation to protect confidentiality.

- 5) **Explore potential confidentiality protections offered by agriculture being declared a Homeland Security Critical Infrastructure.** APHIS is currently working with DHS to assess the implications of the critical infrastructure designation.

#### Ability to share information with an increasing number/diversity of partners

VS' ability to share information with other partners is also determined by the application of the PA and FOIA. Utilizing the "routine use" exception under the PA, VS is able to share information contained within a PA system of records with other governmental and nongovernmental entities (without prior written notification) as stated within the Federal Register notice which outlines the purpose for which the information was collected. (A system of records is a collection/group of records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number or symbol assigned to the individual.) Information shared under the PA may, however, be subject to disclosure under the FOIA.

The PA governs VS' ability to share information about private individuals not businesses. (Note: whether information about farm owners is considered individual or business information is not entirely clear; USDA generally considers farmers and ranchers to be businesses) Disclosing information about businesses is governed by the FOIA. Under the FOIA, VS is not able to make selective disclosures of information; information released to one may be released to all. An exception to this requirement exists for information shared with other federal agencies. Interagency information sharing is generally done for a specific purpose and can generally meet the criteria for Exemption 5 (intra/inter-agency records) under the FOIA. To support an agency's ability to make an Exemption 5 claim, it is important for the agency to: 1) publish the necessary Federal Register notices (FOIA/PA), 2) establish ownership/control; and 3) indicate the intended purpose of the sharing (routine use, official use, investigatory purposes). VS currently lacks Federal Register notices for some of its databases.

VS does not have any current authority to share information selectively with state governments, especially information contained in systems for which VS has not published a Federal Register notice (see discussion below on assuring compliance with privacy/disclosure statutes). VS' current operation of joint information systems with state governments, i.e., EMRS, GDB, etc., likely constitutes a discretionary disclosure under the FOIA even though the states have not filed a FOIA request. As such, should another requestor ask for the information in those databases, VS would likely be compelled to release the same information to other requesters. One exception would be when information is shared with local and state law enforcement agencies as part of an investigation. In addition, in the current homeland security atmosphere, the agency could also try to make the case that, even if the information resides in the public domain, it does not eliminate the possibility that further disclosure could cause harm to protected sources, methods, and/or operations.

Current/potential actions VS is taking/can take –

- 1) **Publish rules detailing how otherwise exempt information can be shared with particular entities** – FDA, FSIS, and the Federal Energy Regulatory Commission (FERC) have each promulgated rules in recent years which establish a procedure for those agencies to share information which would otherwise be exempt from disclosure under FOIA with specific parties without that information being subject to further release (see summary of each rule in Attachment 3). Each of these agencies has taken this step because of the need to work cooperatively with other entities. As the federal register notice announcing FDA's rule states, "*FDA's interaction with State agencies has become more important, particularly as Federal and State authorities have been added....The current degree of Federal-State cooperation was not contemplated back in 1974 when FDA first issued its public information regulations. New Federal laws enacted since 1974 have also emphasized the importance of Federal-State cooperation*" (Federal Register December 8, 1995). The FDA regulation applies to confidential commercial information (except trade secret information concerning manufacturing methods and processes) while the FSIS regulation is limited to just product distribution lists. The FERC regulation applies to critical energy infrastructure information. Parties allowed access to the information by one of these agencies are required to enter into a Memorandum of Understanding or Nondisclosure Agreement. Several states, due to their own freedom of information laws, are unable to sign these MOUs or Nondisclosure Agreements and thus, these published rules have not been a complete solution to this issue for FDA, FSIS, or FERC.
- 2) **Seek legislation specifically allowing the sharing of information and pre-emption of state freedom of information laws.** The Homeland Security Act of 2002 not only exempted critical infrastructure information obtained by DHS from FOIA, it also allows DHS to share this information with state and local governments and other entities without those entities being required to share the information under their own freedom of information laws (i.e., the law pre-empts state freedom of information laws). APHIS would obtain a similar pre-emption for information associated with the animal identification system under Congressional bill H.R. 3787 National Farm Animal Identification and Records Act, which would not only exempt information from the animal identification system from FOIA, but it would also allow the sharing of this information with other parties and would pre-empt state freedom of information laws when the information in question relates to interstate or international commerce. APHIS is also exploring crafting legislation.

#### Assuring VS compliance with relevant privacy/disclosure statutes

VS compliance with the PA and other statutes has lapsed. The PA requires that agencies publish a Federal Register notice when establishing any PA system of records. This notice describes the name and location of the system, the categories of individuals on whom records are maintained in the system, and each routine use of records contained in the system. VS currently has only two published PA notices, one for the old Brucellosis Information System and one for the Veterinary Accreditation System. The language in each of these notices is out of date. Given all

of the new information systems created by VS, it appears that VS needs to examine each of these new systems and determine if additional PA notices are required.

VS must also develop processes to achieve compliance with the new requirements for conducting Privacy Impact Assessments (PIA). A PIA is required: before developing or procuring IT systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public; initiating a new electronic collection of information in identifiable form for 10 or more persons; or where a system change creates new privacy risks. In a PIA the agency analyzes how information is handled to: ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. It is not clear within VS who is responsible for producing PIAs.

Current/potential actions VS is taking/can take –

- 1) **Develop and publish Federal Register notices for all VS PA system of records and revise those notices which are outdated.** Bringing VS into compliance with the PA requirements may strengthen the agency's ability to apply various exceptions and exemptions for withholding information and/or selectively sharing information.
- 2) **Create a process for ensuring that the required PA notices are published when new systems are established.** Development of PA notices should be included in the steps for starting new programs and staff officers should be educated on the requirements.
- 3) **Ensure that required Privacy Impact Assessments are being conducted for IT systems.** The PIA requirement must be incorporated into the existing procedures for creating/modifying systems. VS must clearly establish who is responsible for carrying out PIAs.

### **Proposed Actions:**

As mentioned earlier, the Animal Health Safeguarding Review made no specific proposals regarding confidentiality. The Information Technology Issue Group finds that there are a number of actions VS can take to improve its ability to protect confidential information, but there is no one approach that will resolve all confidentiality issues. Therefore, the Information Technology Issue Group recommends that VS establish a Confidentiality Task Force to: 1) thoroughly review the types of information VS collects, 2) assess the sensitivity of the information regarding the risk of disclosure and the impact of disclosure on cooperation, 3) evaluate options for maintaining confidentiality of sensitive information, 4) develop a comprehensive strategy for addressing confidentiality of all types of information collected by VS, and 5) ensure that VS is in full compliance with all relevant statutes for the information it collects and maintains.

## Implementation Plan:

### Tasks

- 1) Establish a Confidentiality Task Force. The task force should have representation from VS units involved in all major information collection efforts, LPA FOIA staff, PPD Regulatory Analysis and Development staff, and OGC/General Law Division. (Task Force should be established within 1 month of VSMT approval of this action plan, July 2004)
- 2) Task Force identifies: types of information VS is collecting or planning to collect, linkages between information systems, current privacy or confidentiality requirements for each type of information, and current compliance with required Federal Register notices.
- 3) Task Force develops a comprehensive strategy for improving VS' ability to instill confidence in data providers and in being able to share information with key partners.
- 4) Task Force strategic plan is provided to VSMT for review and approval. (Task Force should submit its strategic plan within 4 months after being established, November 2004)
- 5) Following VSMT approval, Task Force initiates rulemaking processes for Federal Register notices and drafting of MOUs as needed for partners with which VS intends to share information. Task Force also drafts language to be used by producers and other entities when submitting information voluntarily to the agency.

Accountable Individual/Group The VSMT is responsible for establishing the Confidentiality Task Force, members of the Task Force are responsible for carrying out the actions.

Other Key Players VS offices with major data collection efforts such as CEAH, CVB, EMS, MSS, NAHPP, NVSL, and Regional offices.

Resources Needed Staff time to devote to task force work and travel funds to attend meetings (travel costs \$10,000).

Statutory/Regulatory Impacts It is likely that the work of the Task Force will result in APHIS rulemaking and/or Congressional action.

Political Sensitivities Confidentiality concerns are a key interest of industry groups and state government officials. Proposals to limit the access of the public to information collected by VS will be scrutinized carefully by other interest groups. Any proposal which recommends pre-emption of state laws will be controversial.

Sequencing Confidentiality concerns need to be addressed before a new national surveillance system can be fully realized. Confidentiality concerns can also hamper the establishment of a National Animal Health Laboratory Network.

**Partnering/Cooperation/Communication:** Clarification of confidentiality procedures could improve partnering/cooperation/communication between VS and its state and industry partners.

However, it is unlikely that VS will be able to fully address all of the confidentiality concerns to the degree that these partners desire which could result in continued tensions.

**Expected Outcome and Performance Indicators:** If successfully implemented, this action plan will result in VS developing a comprehensive confidentiality plan for all its information systems. VS will also improve its compliance with all relevant privacy and confidentiality statutes. Achieving these goals will allow VS to meet its performance goals for surveillance and formation of the laboratory network.

**Linkage to the VS Strategic Plan:** Addressing confidentiality concerns will allow VS to move forward on major initiatives in the development of a comprehensive national surveillance system and in the development of a national animal health laboratory network.

**Attachment 1:  
VS Information Systems Containing Information on Individuals or  
Businesses\***

<b>System</b>	<b>Description and Principal Data Elements</b>
Adverse Event Reporting	System tracks adverse events potentially connected with the use of veterinary biologics. The focus of the system is on the particular biologics product involved in the event. The database contains name and address information about the veterinarian administering the product, animal owners name and address (if relevant), product administered and details about the adverse event observed.
Emergency Management Response System	System tracks data needed to manage emergency response activities. Separate databases are contained in the system for specific response efforts (i.e., BSE in Washington state and END in Western states). Databases are also available for foreign and emerging disease investigations. The database contains: premises identification number, animal owners name and address (can be private individuals or businesses), details about the disease investigation, test results, details about any actions taken on the premises (such as euthanasia and disposal, cleaning and disinfection, appraisal), and geographic coordinates for the premises.
Export Health Certification System	System tracks export health certificates issued for live animals and animal products. The database contains information about the animals and products to be exported, consignor's name and address, signing veterinarian's name and address, animal owner's name and address, test results, and laboratory name.
Generic Disease Database	System tracks status of herds involved in VS programs such as brucellosis, chronic wasting disease Johnes, pseudorabies, and tuberculosis. The system also tracks geospatial and capacity data for livestock concentration points (markets, slaughter plants) as part of the national mapping effort. The database contains name and address information for the herd owner, geographic coordinates, premises identification number, status of the herd, pending certifications, tests run on the herd, test results, and details about actions taken on the herd (euthanasia, cleaning and disinfection).
High Consequence Agent Registration and Tracking System	System registers and tracks facilities and individuals with access to specific high consequence agents. Database contains names and addresses of registered individuals and facilities, high consequence agents the individual/facility has access to, and information about inspections performed on the facility.
Import Authorization System	System tracks applications for import permits for animals and animal products. Database contains names and addresses of importers and shippers, type of material being imported, treatments proposed for the material, final disposition of the imported material, date of import, and port of entry.
Import Tracking System	System is designed to track imports of live animals (and a few animal products) into the United States. The database contains names and addresses of importers who may be individuals or businesses, names and addresses of destination which may also be individuals or businesses, type and number of live animals imported.
Interstate Certificate of Veterinary Inspection	System tracks interstate health certificates issued for live animals and animal products. The database contains information about the animals and products to be shipped interstate, consignor's name and address, signing veterinarian's name and address, animal owner's name and address, test results, and laboratory name.
Johnes Demo Herd Database (temporary)	Database tracks management practice information and test results for herds participating in the demonstration project.
Licensing, Serial Release, Testing, Inspection System	System tracks licensing of biologics; serial release will be incorporated into this system but is not initiated yet. The database contains information regarding biologics firms including licensing, products, labels, and key personnel. Information maintained on key personnel includes: name, job title, contact information, years employed at the firm, and degree.

<b>System</b>	<b>Description and Principal Data Elements</b>
National Animal Health Laboratory Network	System will identify laboratories that are certified to provide diagnostic tests. System will have the capability to merge test results obtained at these laboratories into the national response system. For diagnostic tests conducted, the system will contain premises identification numbers, sample identification numbers, submitter's name, and test results. The owner's name and address will be included in the system until the premises allocator is available.
National Animal Health Monitoring Surveys	NAHMS collects information on management practices in US livestock industries. The individual survey databases contain information about individual operations but these operations are identified only by an identification number. The types of information collected include: demographic information about the operation, details about a variety of management practices, and results of any diagnostic tests conducted on the operation.
NAHRMS**	System tracks antimicrobial resistance test results for samples collected by USDA and HHS. Agencies in both departments access the system. The database contains plant identification numbers, collection data, species, and test results.
National Poultry Improvement Plan	System tracks information about flocks enrolled in the NPIP. Database contains name and address information for the flock, information about tests performed on the flock, and details about the flocks certification status.
Veterinary Accreditation	System tracks accreditation status of veterinarians. Database contains name and address of the accredited veterinarian, training completed, and information about violations.
Veterinary Biologics Information System	Database is used for regulatory purposes for veterinary biologics serial release. The database contains firm establishment addresses and outdated information about firm personnel including role, degree held, and business telephone number.

\* This table focuses on databases which track information on businesses and individuals. VS also maintains other databases, such as the National Animal Health Reporting System, which contain sensitive information about individual states.

\*\* Ownership/control of the NAHRSM may not belong to APHIS; ownership/control needs to be clarified with ARS, FDA, and FSIS.

## **Attachment 2: Summary of Federal Laws and other Rules affecting Confidentiality**

### **Privacy Act 1974**

“Broadly stated, the purpose of the Privacy Act (PA) is to balance the government’s need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from federal agencies’ collection, maintenance, use, and disclosure of personal information about them.” (DOJ) The PA governs the collection, use, and sharing of information by the federal government about individuals and requires agencies to safeguard identifiable information. A system of records is defined in the PA as any group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. Agencies cannot disclose information about an individual contained in a system of records to another person or agency without prior written consent of the individual unless the disclosure is authorized by law. There are 12 exceptions under which an agency may disclose information without consent. The most significant exception for APHIS is routine use which allows the agency to share information with other federal agencies, and state, local and tribal governments without prior written consent when the disclosure is for a purpose which is compatible with the purpose for which the information was collected. (Note: The PA only covers information about individuals not businesses, so the routine use exception does not address APHIS’ selective sharing of information about businesses). The PA grants individuals the right to access records the agency maintains on them and the right to amend the record if it is inaccurate, irrelevant, untimely or incomplete. PA also requires that the federal government inform the public of the existence of systems of records containing personal information.

### **Freedom of Information Act**

The FOIA provides for public access to federal agency records. The FOIA firmly establishes a statutory right of public access to executive branch information. The Act operates through an exemption structure to “strike a balance between information disclosure and nondisclosure, with an emphasis on the fullest responsible disclosure” (DOJ, Freedom of Information Act Guide May 2002). The FOIA exemptions are discretionary not mandatory and agencies are allowed to make discretionary disclosures of exempt information. However, once information is disclosed to one requestor, it must be disclosed to all. Agency decisions to withhold information based on the nine exemptions provided in the Act are subject to legal challenge. The most relevant exemptions for APHIS are discussed below:

Exemption 1 protects from disclosure national security information concerning the national defense or foreign policy, provided that the information has been properly classified in accordance with the substantive and procedural requirements of an executive order.

Exemption 2 exempts from mandatory disclosure records that are related solely to the internal personnel rules and practices of an agency. Exemption 2 has also been applied to internally held information which could be used to circumvent an agency regulation or statute. A FOIA

disclosure should not benefit those attempting to violate the law and avoid detection. Information about vulnerability assessments has been deemed to be covered by Exemption 2. Covered vulnerability assessments include those which assess an agency's vulnerability (or that of another institution) to some form of outside interference or harm by identifying those programs or systems deemed the most sensitive and describing specific security measures that can be used to counteract such vulnerabilities. The White House has encouraged that agencies avail themselves of the full measure of protection provided for critical infrastructure information under Exemption 2.

Exemption 3 covers exemptions provided by other statutes such as the Homeland Security Act for the Department of Homeland Security and the Agricultural Bioterrorism Act for APHIS.

Exemption 4 protects trade secrets and commercial or financial information obtained from a person that is privileged or confidential. This exemption protects the interests of both the government and submitters by both encouraging submitters to voluntarily furnish reliable information to the government and protecting commercial and financial information required by the government from being disclosed. Two broad categories of information are covered by this exemption: 1) trade secrets and 2) commercial or financial information that is privileged or confidential. "Trade secret protection has been recognized for product manufacturing and design information, but has been denied for general information concerning a product's physical or performance characteristics or a product formula when release would not reveal the actual formula itself." (DOJ, FOIA Guide May 2002, Exemption 4). The Trade Secrets Act overlaps with the provisions of FOIA Exemption 4 but has the effect of limiting an agency's ability to make a discretionary disclosure of otherwise exempt material. Information is considered "confidential" for the purposes of Exemption 4 if "disclosure of the information is likely to have either of the following effects: 1) impair the Government's ability to obtain necessary information in the future; or 2) cause substantial harm to the competitive position of the person from whom the information was obtained." (DOJ, FOIA Guide May 2002, Exemption 4). Voluntarily provided information is protected if it is not information customarily disclosed to the public by the submitter. Competitive harm decisions have been judged on a case-by-case basis and the release of similar information may be treated differently in separate cases. Competitive harm is limited to "harm flowing from the affirmative use of propriety information by competitors and this "should not be taken to mean simply any injury to competitive position, as might flow from customer or employee disgruntlement" (DOJ, FOIA Guide May 2002, Exemption 4). Examples of information for which disclosure might pose competitive harm include: detailed financial information such as a company's assets, liabilities, and net worth; a company's actual costs, breakeven calculations, profits, and profit rates; data describing a company's workforce which would reveal labor costs, profit margins, and competitive vulnerability; a company's selling prices, purchase activity, and freight charges; a company's purchase records; technical and commercial data, names of consultants, and subcontractors, performance, cost and equipment information; shipper and importer names, type and quantity of freight hauled, routing systems, cost of raw materials; currently unannounced and future products, proprietary technical information, pricing strategy and subcontractor information; raw research data used to support a pharmaceutical drug's safety and effectiveness; information regarding an unapproved application to market the drug in a different manner, and sales and distribution data of a drug manufacturer; and technical proposals which are submitted, or could

be used, in conjunction with offers on government contracts (DOJ, FOIA Guide May 2004, Exemption 4). “Executive Order 12600 provides for mandatory notification of submitters of confidential commercial information whenever an agency “determines that it may be required to disclose” such information under the FOIA.” Also protected are records that are “intrinsically valuable”, i.e., significant not for their content but as valuable commodities which can be sold in the marketplace.

Exemption 5 protects inter-agency or intra-agency memorandums or letters which are part of the deliberative process of an agency. If a document is immune from civil discovery, it is similarly protected from mandatory disclosure under the FOIA.

Exemption 6 permits the government to withhold information about individuals contained in personnel and medical files and similar files when disclosure of that information would “constitute a clearly unwarranted invasion of personal privacy”. To be protected under Exemption 6, the information must be identifiable to a specific individual and the privacy interest in nondisclosure must outweigh any public interest in disclosure.

### **Trade Secrets Act**

The Trade Secrets Act makes it a crime for an officer or employee of the United States or any department or agency thereof, to disclose or make known in any manner or to any extent not authorized by law any information coming to him in the course of his employment or official duties which concerns or relates to the trade secrets, processes, operations, style of work, or apparatus, or to the identity, confidential statistical data, amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation, or association.

### **Computer Security Act 1987**

The Computer Security Act provides for improving the security and privacy of sensitive information in federal computer systems where sensitive information includes any unclassified information that, if lost, misused or accessed or modified without authorization, could adversely affect the national interest, conduct of federal programs, or the privacy to which individuals are entitled under the Privacy Act. Under the Act, agencies are required to develop plans for the security and privacy of sensitive information in federal computer systems.

### **Paperwork Reduction Act 1995**

The Paperwork Reduction Act requires OMB to provide central guidance for and oversight of federal agencies’ information management activities including those under the PA. The Paperwork Reduction Act also requires federal agencies to ensure compliance with the PA and coordinate management of the requirements of the FOIA, the PA, the Computer Security Act and related information management laws. The Paperwork Reduction Act also requires agencies to “implement and enforce applicable policies, procedures, standards, and guidelines on privacy, confidentiality, security, disclosure and sharing of information collected or maintained by or for the agency”.

## **OMB Order Providing for the Confidentiality of Statistical Information June 1997**

The order was issued by OMB to clarify and make consistent government policy protecting the privacy and confidentiality interests of individuals or organizations who furnish data for Federal statistical programs. It is intended to assure respondents who supply statistical information needed to develop or evaluate Federal policy that their responses will be held in confidence and will not be used against them in any government action. In effect, it clarifies and amplifies the privileged status afforded confidential statistical data about businesses and organizations as set forth in the Trade Secrets Act as well as the principles of the PA concerning information about individuals. The order permits functional separation to be achieved by two means – 1) identifying an agency or unit that is purely statistical and 2) distinguishing statistical from non-statistical functions within a single agency or unit.

The order lists a number of agencies or units that have been determined by OMB to be statistical agencies or units (longer list than under the Confidential Information Protection and Statistical Efficiency Act (see E Government Act of 2002 below)).

## **E-Government Act of 2002**

The E-Government Act of 2002 aims to enhance the management and promotion of electronic government services and processes. The Act also contains several important provisions related to privacy and confidentiality. The Act sets forth a requirement for agencies to conduct Privacy Impact Assessments when developing or procuring IT systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public or initiate new electronic collection of information in identifiable form for 10 or more persons. PIAs are also required when IT systems are changed in ways which create new privacy risks such as when agencies begin to employ new relational database technologies to access multiple data stores.

Title V of the E-government Act of 2002 is also known as the Confidential Information Protection and Statistical Efficiency Act (CIPSEA). CIPSEA is designed to protect the confidentiality of certain types of data across the government and allows key statistical agencies to share business data. Two main functions of the Act are to: 1) ensure that information supplied by individuals or organizations to an agency for statistical purposes under a pledge of confidentiality is used exclusively for statistical purposes and 2) to authorize the sharing of business data among the Bureau of the Census, the Bureau of Economic Analysis, and the Bureau of Labor Statistics for exclusively statistical purposes. The Act defined non-statistical purposes to include using information for administrative, regulatory, law enforcement, judicial, or other purposes that may affect the rights, privileges, or benefits of a respondent. OMB expected to issue guidance on the Act by late 2003 or early 2004.

The Act designated three agencies as statistical agencies – Bureau of Labor Statistics, Census Bureau, and Bureau of Economic Analysis. These agencies need written agreements with each other to share information. Statistical agencies or units may designate agents, by contract or by entering into a special agreement containing the provisions required for treatment as an agent, who may perform exclusively statistical activities, subject to the limitations and penalties described in the Act.

**Public Health Security and Bioterrorism Preparedness and Response Act of 2002  
(including Agricultural Bioterrorism Protection Act of 2002)**

The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 sets forth some disclosure guidelines for information pertaining to biological agents and toxins. The following information cannot be disclosed under FOIA: 1) any registration or transfer documentation submitted or permits issued prior to the enactment of the Act for the possession, use, or transfer of a listed agent or toxin, or information derived therefrom to the extent that it identifies the listed agent or toxin possessed, used or transferred by a specific person or discloses the identity or location of a specific person, 2) the national database or any compilation of the registration or transfer information to the extent that such compilation discloses site-specific registration or transfer information, 3) any portion of a record that discloses the site-specific or transfer-specific safeguard and security measures used by a registered person to prevent unauthorized access to listed agents and toxins, 4) any notification of a release of a listed agent or toxin or any notification of theft or loss, and 5) any portion of an evaluation or report of an inspection that identifies the listed agent or toxin possessed by a specific registered person or that discloses the identify or location of a specific registered person if the agency determines that public disclosure of the information would endanger public health or safety. (Title II, Section 351A and Subtitle B, Sec 212, Disclosure of Information)

## **Attachment 3: Agency Specific Statutes/Rules Guiding Confidentiality**

### **The Homeland Security Act of 2002**

The Homeland Security Act of 2002 contained provisions for exempting critical infrastructure information from disclosure under the FOIA. Under Subtitle B of the Act (named Critical Infrastructure Information Act of 2002), “critical infrastructure information that is voluntarily submitted to a covered agency for use by that agency regarding the security of critical infrastructure” is exempt from disclosure under the FOIA if that information is accompanied by a written marking to the effect that “this information is voluntarily submitted to the federal government in expectation of protection from disclosure”. The only covered agency is the Department of Homeland Security. Critical infrastructure information includes:

- actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure by either physical or computer-based attack that violates federal or state law, harms interstate commerce, or threatens public health and safety;
- the ability of critical infrastructures to resist such attacks;
- any planned or past operational problem or solution regarding critical infrastructure including repair, recovery, reconstruction, insurance, or continuity to the extent it relates to such interference, compromise, or incapacitation.

The Act also states that if the critical infrastructure information is disclosed to state or local officials, it may not be used for any purpose other than the protection of critical infrastructures, and it may not be disclosed under state disclosure laws, i.e., state disclosure laws are pre-empted by the Act.

In February 2004, DHS issued an interim rule implementing procedures for handling critical infrastructure information. The rule distinguishes critical infrastructure information from protected critical infrastructure information and establishes more detailed requirements for information to be categorized as protected critical infrastructure information. Among those requirements is that the information be voluntarily provided and not customarily in the public domain. The submitter must certify that the information is not being submitted in lieu of independent compliance with a federal legal requirement and the submitter must note any information being submitted which is required to be submitted to another federal agency. Protected critical infrastructure information provided by DHS to other federal agencies or to state and local governments, can only be used for the purpose of securing the critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, restitution, or other informational purpose including the identification, analysis, prevention, preemption, and/or disruption of terrorist threats. Written agreements will be required between DHS and those federal, state, and local government agencies which would like to have access to protected critical infrastructure information.

## **Transportation Security Administration, Sensitive Security Information Final Rule, February 2002**

The Transportation Security Administration issued a rule in February 2002 which prohibits disclosure of sensitive security information which includes information such as security programs and procedures of airport and aircraft operators, procedures TSA uses to perform security screening, and information detailing vulnerabilities in the aviation system or a facility. TSA's authority to designate information as sensitive security information is derived from 49 USC 114. The SSI Statute creates a statutory exemption to the general disclosure requirements of FOIA. TSA shares sensitive security information with persons with a need to know in order to carry out transportation security duties. This includes persons both within and outside the Federal government.

### **FDA regulations 21 CFR 20.85 and 20.88**

FDA has language in its regulations allowing the disclosure of confidential commercial information and predecisional documents to state government officials under certain conditions. Such information will only be shared with states who have the authority to protect this information from disclosure and who commit to not disclose any such information without the written permission of the submitter or FDA. Disclosure of trade secret information concerning manufacturing methods and processes is not allowed. Sharing of confidential commercial information and predecisional documents with state officials does not invoke a requirement to make these records available to all members of the public. Sharing of confidential commercial information is in the interest of public health by reason of the "State government's possessing information concerning the safety, effectiveness, or quality of a product or information concerning an investigation or by reason of the State government being able to exercise its regulatory authority more expeditiously than the FDA". Sharing of predecisional documents is in the interest of improving Federal-State uniformity, cooperative regulatory activities, or implementation of Federal-State agreements.

### **FSIS Sharing Recall Distribution Lists with States and Other Federal Government Agencies**

FSIS issued a final rule in April 2002 establishing regulations for sharing distribution lists from a firm that is recalling meat or poultry products with state and other federal agencies. FSIS declares that this rule will permit FSIS to share these lists without being compelled to disclose the information to the public under the FOIA. These product distribution lists would otherwise be considered confidential business information and exempt under FOIA exemption 4, however, FSIS asserts that protecting the public health is served by allowing the agency to share this information. FSIS will only share these distribution lists with those states that can provide a written statement establishing their authority to protect distribution lists from public disclosure and a written commitment not to disclose such information without the submitter's written permission. Officials of other federal agencies must provide a similar written commitment not to disclose the information and must refer any requests for distribution lists to FSIS for response. Depending on their own freedom of information laws, not all states can enter into these written agreements and so FSIS is still limited in the extent to which it can share these distribution lists.

## **Federal Energy Regulatory Commission, Critical Energy Infrastructure Information Final Rule February 2003**

In February 2003, the Federal Energy Regulatory Commission issued a final rule establishing a procedure for allowing access to critical energy infrastructure information that would otherwise not be available under the FOIA. FERC established this separate process because of limitations in using the FOIA process for handling requests for critical energy infrastructure information: 1) information considered to be critical energy infrastructure information is generally protected from disclosure under FOIA, 2) under FOIA, an agency may not distinguish among requesters based on their particular need for the information; information given to one FOIA requestor must be given to all requestors, and 3) the agency may not restrict the recipient's use or dissemination of information provided under FOIA. In order to qualify for protection as critical energy infrastructure information, the information must relate to the production, generation, transportation, transmission, or distribution of energy; be useful to terrorists in planning an attack; be exempt from disclosure under the FOIA; and not merely give the location of the infrastructure. Release of critical energy infrastructure information to state commissions or agencies will be subject to signing of a non-disclosure agreement. Other types of entities that might also be able to request critical energy infrastructure information include interveners, market participants, energy market consultants, state agencies, landowners, and environmental groups. Some of the information now being protected as critical energy infrastructure information used to be provided routinely by FERC to the public prior to September 11<sup>th</sup>.