Terminology and Other Government Designations

Several discussions or definitions related to this issue are provided below:

- **Section 147, "Safeguards Information," of the Atomic Energy Act, as amended, 42 USC §2167, states:**

  a. In addition to any other authority or requirement regarding protection from disclosure of information, and subject to subsection (b)(3) of section 552 of title 5, the Commission shall prescribe such regulations, after notice and opportunity for public comment, or issue such orders, as necessary to prohibit the unauthorized disclosure of safeguards information which specifically identifies a licensee's or applicant's detailed -

  (1) control and accounting procedures or security measures (including security plans, procedures, and equipment) for the physical protection of special nuclear material, by whomever possessed, whether in transit or at fixed sites, in quantities determined by the Commission to be significant to the public health and safety or the common defense and security;

  (2) security measures (including security plans, procedures, and equipment) for the physical protection of source material or byproduct material, by whomever possessed, whether in transit or at fixed sites, in quantities determined by the Commission to be significant to the public health and safety or the common defense and security; or

  (3) security measures (including security plans, procedures, and equipment) for the physical protection of and the location of certain plant equipment vital to the safety of production or utilization facilities involving nuclear materials covered by paragraphs (1) and (2) if the unauthorized disclosure of such information could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of theft, diversion, or sabotage of such material or such facility. The Commission shall exercise the authority of this subsection -

  (A) so as to apply the minimum restrictions needed to protect the health and safety of the public or the common defense and security, and

  (B) upon a determination that the unauthorized disclosure of such information could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of theft, diversion, or sabotage of such material or such facility.

- **§ 73.2 Title 10 of Code Federal Regulations**

  Safeguards Information means information not otherwise classified as National Security Information or Restricted Data which specifically identifies a licensee's or applicant's detailed, (1) security measures for the physical protection of special nuclear material, or (2) security measures for the physical protection and location of certain plant equipment vital to the safety of production or utilization facilities.

- **§ 73.21 Title 10 of Code Federal Regulations**

  (b) *Information to be protected*. The specific types of information, documents, and reports that shall be protected are as follows:
  (1) *Physical protection at fixed sites*. Information not otherwise classified as Restricted Data or National Security Information relating to the protection of facilities that possess formula quantities of strategic special nuclear material, and power reactors. Specifically:
  (i) The composite physical security plan for the nuclear facility or site.
  (ii) Site specific drawings, diagrams, sketches, or maps that substantially represent the final design features of the physical protection system.
  (iii) Details of alarm system layouts showing location of intrusion detection devices, alarm assessment equipment, alarm system wiring, emergency power sources, and duress alarms.
  (iv) Written physical security orders and procedures for members of the security organization, duress codes, and patrol schedules.
  (v) Details of the on-site and off-site communications systems that are used for security purposes.
  (vi) Lock combinations and mechanical key design.
  (vii) Documents and other matter that contain lists or locations of certain safety-related equipment explicitly identified in the documents as vital for purposes of physical protection, as contained in physical security plans, safeguards contingency plans, or plant specific safeguards analyses for production or utilization facilities.
  (viii) The composite safeguards contingency plan for the facility or site.
  (ix) Those portions of the facility guard qualification and training plan which disclose features of the physical security system or response procedures.
  (x) Response plans to specific threats detailing size, disposition, response times, and armament of responding forces.
  (xi) Size, armament, and disposition of on-site reserve forces.
  (xii) Size, identity, armament, and arrival times of off-site forces committed to respond to safeguards emergencies.
  (xiii) Information required by the Commission pursuant to 10 CFR 73.55 (c) (8) and (9).

(2) *Physical protection in transit*. Information not otherwise classified as Restricted Data or National Security Information relative to the protection of shipments of formula quantities of strategic special nuclear material and spent fuel. Specifically:
(i) The composite transportation physical security plan.
(ii) Schedules and itineraries for specific shipments. (Routes and quantities for shipments of spent fuel are not withheld from public disclosure. Schedules for spent fuel shipments may be released 10 days after the last shipment of a current series.)
(iii) Details of vehicle immobilization features, intrusion alarm devices, and communication systems.
(iv) Arrangements with and capabilities of local police response forces, and locations of safe havens.
(v) Details regarding limitations of radio-telephone communications.
(vi) Procedures for response to safeguards emergencies.
(3) *Inspections, audits and evaluations*. Information not otherwise classified as National Security Information or Restricted Data relating to safeguards inspections and reports. Specifically:
(i) Portions of safeguards inspection reports, evaluations, audits, or investigations that contain details of a licensee's or applicant's physical security system or that disclose uncorrected defects, weaknesses, or vulnerabilities in the system. Information regarding defects, weaknesses or vulnerabilities may be released after corrections have been made. Reports of investigations may be released after the investigation has been completed, unless withheld pursuant to other authorities, e.g., the Freedom of Information Act (5 U.S.C. 552).
(4) *Correspondence*. Portions of correspondence insofar as they contain Safeguards Information specifically defined in paragraphs (b)(1) through (b)(3) of this paragraph.

- **Critical Infrastructure Information is defined in Title 6 CFR Part 29 as:**

Critical Infrastructure Information, or CII means information not customarily in the public domain and related to the security of critical infrastructure or protected systems. CII consists of records and information concerning: (1) Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms the interstate commerce of the United States, or threatens public health or safety; (2) The ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation, risk-management planning, or risk audit; or (3) Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

- **Protected CII is defined in Title 6 CFR Part 29 as:**

  Protected Critical Infrastructure Information, or Protected CII means CII (including the identity of the submitting person or entity) that is voluntarily submitted to DHS for its use regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement as described in Sec. 29.5. This information maintains its protected status unless DHS's Protected CII Program Manager or the Protected CII Program Manager's designees render a final decision that the information is not Protected CII.

- **Homeland Security Information is defined in Section 892(f)(1) of the Homeland Security Act of 2002, 6 USC 482, as:**

  any information possessed by Federal, State, or local agency that:
  (A) relates to the threat of terrorist activity;
  (B) relates to the ability to prevent, interdict, or disrupt terrorist activity;
  (C) would improve the identification or investigation of a suspected terrorist or terrorists organization; or
  (D) would improve the response to a terrorist act."

- **Sensitive Homeland Security Information**

  The Department of Homeland Security continues to develop guidance related to sensitive homeland security information (SHSI). The staff will continue to monitor the DHS activities in this area. The definition is expected to be related to the definition of homeland security information provided above. The designation of information as SHSI would be expected to help protect the information from public disclosure while also maintaining the free flow of such information between Federal, State, and Local governments.

- **Critical Energy Infrastructure Information**

  The Federal Energy Regulatory Commission has provided a definition of Critical Energy Infrastructure Information in their regulations at 18 CFR Parts 375 and 388. § 388.113 states :

  (1) Critical energy infrastructure information means information about proposed or existing critical infrastructure that: (i) Relates to the production, generation, transportation, transmission, or distribution of energy; (ii) Could be useful to a person in planning an attack on critical infrastructure; (iii) Is exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. 552; and (iv) Does not simply give the location of the critical infrastructure.

- **Sensitive Security Information (Transportation)**

  The Transportation Safety Administration and Department of Transportation have provided the following definition of "sensitive security information" or SSI in their regulations at 49 CFR Part 15. See interim final rule published May 18, 2004 (69 FR 28066).
  Sec. 15.5 Sensitive security information.
  (a) In general. In accordance with 49 U.S.C. 40119(b)(1), SSI is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which the Secretary of DOT has determined would-- (1) Constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file); (2) Reveal trade secrets or privileged or confidential information obtained from any person; or (3) Be detrimental to transportation safety. (b) Information constituting SSI. Except as otherwise provided in writing by the Secretary of DOT in the interest of public safety or in furtherance of transportation security, the following information, and records containing such information, constitute SSI:
  (1) Security programs and contingency plans. Any security program or security contingency plan issued, established, required, received, or approved by DOT or DHS, including-- (i) Any aircraft operator or airport operator security program or security contingency plan under this chapter; (ii) Any vessel, maritime facility, or port area security plan required or directed under Federal law; (iii) Any national or area security plan prepared under 46 U.S.C. 70103; and (iv) Any security incident response plan established under 46 U.S.C. 70104.
  (2) Security Directives. Any Security Directive or order-- (i) Issued by TSA under 49 CFR 1542.303, 1544.305, or other authority; (ii) Issued by the Coast Guard under the Maritime Transportation Security Act, 33 CFR part 6, or 33 U.S.C. 1221 et seq. related to maritime security; or (iii) Any comments, instructions, and implementing guidance pertaining thereto.
  (3) Information Circulars. Any notice issued by DHS or DOT regarding a threat to aviation or maritime transportation, including any-- (i) Information Circular issued by TSA under 49 CFR 1542.303 or 1544.305, or other authority; and (ii) Navigation or Vessel Inspection Circular issued by the Coast Guard related to maritime security.
  (4) Performance specifications. Any performance specification and any description of a test object or test procedure, for-- (i) Any device used by the Federal government or any other person pursuant to any aviation or maritime transportation security requirements of Federal law for the detection of any weapon, explosive, incendiary, or destructive device or substance; and (ii) Any communications equipment used by the Federal government or any other person in carrying out or complying with any aviation or maritime transportation security requirements of Federal law.
  (5) Vulnerability assessments. Any vulnerability assessment directed, created, held, funded, or approved by the DOT, DHS, or that will be provided to DOT or DHS in support of a Federal security program.

(6) Security inspection or investigative information. (i) Details of any security inspection or investigation of an alleged violation of aviation or maritime transportation security requirements of Federal law that could reveal a security vulnerability, including the identity of the Federal special agent or other Federal employee who conducted the inspection or audit. (ii) In the case of inspections or investigations performed by TSA, this includes the following information as to events that occurred within 12 months of the date of release of the information: the name of the airport where a violation occurred, the airport identifier in the case number, a description of the violation, the regulation allegedly violated, and the identity of any aircraft operator in connection with specific locations or specific security procedures. Such information will be released after the relevant 12-month period, except that TSA will not release the specific gate or other location on an airport where an event occurred, regardless of the amount of time that has passed since its occurrence. During the period within 12 months of the date of release of the information, TSA may release summaries of an aircraft operator's, but not an airport operator's, total security violations in a specified time range without identifying specific violations or locations. Summaries may include total enforcement actions, total proposed civil penalty amounts, number of cases opened, number of cases referred to TSA or FAA counsel for legal enforcement action, and number of cases closed.
(7) Threat information. Any information held by the Federal government concerning threats against transportation or transportation systems and sources and methods used to gather or develop threat information, including threats against cyber infrastructure.
(8) Security measures. Specific details of aviation or maritime transportation security measures, both operational and technical, whether applied directly by the Federal government or another person, including-- (i) Security measures or protocols recommended by the Federal government; (ii) Information concerning the deployments, numbers, and operations of Coast Guard personnel engaged in maritime security duties and Federal Air Marshals, to the extent it is not classified national security information; and (iii) Information concerning the deployments and operations of Federal Flight Deck Officers, and numbers of Federal Flight Deck Officers aggregated by aircraft operator. (9) Security screening information. The following information regarding security screening under aviation or maritime transportation security requirements of Federal law: (i) Any procedures, including selection criteria and any comments, instructions, and implementing guidance pertaining thereto, for screening of persons, accessible property, checked baggage, U.S. mail, stores, and cargo, that is conducted by the Federal government or any other authorized person. (ii) Information and sources of information used by a passenger or property screening program or system, including an automated screening system. (iii) Detailed information about the locations at which particular screening methods or equipment are used, only if determined by TSA to be SSI. (iv) Any security screener test and scores of such tests. (v) Performance or testing data from security equipment or screening systems. [[Page 28080]] (vi) Any electronic image shown on any screening equipment monitor, including threat images and descriptions of threat images for threat image projection systems.
(10) Security training materials. Records created or obtained for the purpose of training persons employed by, contracted with, or acting for the Federal government or another person to carry out any aviation or maritime transportation security measures required or recommended by DHS or DOT.

(11) Identifying information of certain transportation security personnel. (i) Lists of the names or other identifying information that identify persons as-- (A) Having unescorted access to a secure area of an airport or a secure or restricted area of a maritime facility, port area, or vessel or; (B) Holding a position as a security screener employed by or under contract with the Federal government pursuant to aviation or maritime transportation security requirements of Federal law, where such lists are aggregated by airport; (C) Holding a position with the Coast Guard responsible for conducting vulnerability assessments, security boardings, or engaged in operations to enforce maritime security requirements or conduct force protection; (D) Holding a position as a Federal Air Marshal; or (ii) The name or other identifying information that identifies a person as a current, former, or applicant for Federal Flight Deck Officer.
(12) Critical aviation or maritime infrastructure asset information. Any list identifying systems or assets, whether physical or virtual, so vital to the aviation or maritime transportation system that the incapacity or destruction of such assets would have a debilitating impact on transportation security, if the list is-- (i) Prepared by DHS or DOT; or (ii) Prepared by a State or local government agency and submitted by the agency to DHS or DOT.
(13) Systems security information. Any information involving the security of operational or administrative data systems operated by the Federal government that have been identified by the DOT or DHS as critical to aviation or maritime transportation safety or security, including automated information security procedures and systems, security inspections, and vulnerability information concerning those systems.
(14) Confidential business information. (i) Solicited or unsolicited proposals received by DHS or DOT, and negotiations arising therefrom, to perform work pursuant to a grant, contract, cooperative agreement, or other transaction, but only to the extent that the subject matter of the proposal relates to aviation or maritime transportation security measures; (ii) Trade secret information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying out aviation or maritime transportation security responsibilities; and (iii) Commercial or financial information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying out aviation or maritime transportation security responsibilities, but only if the source of the information does not customarily disclose it to the public.
(15) Research and development. Information obtained or developed in the conduct of research related to aviation or maritime transportation security activities, where such research is approved, accepted, funded, recommended, or directed by the DHS or DOT, including research results.
(16) Other information. Any information not otherwise described in this section that TSA determines is SSI under 49 U.S.C. 114(s) or that the Secretary of DOT determines is SSI under 49 U.S.C. 40119. Upon the request of another Federal agency, the Secretary of DOT may designate as SSI information not otherwise described in this section.

- **Sensitive Security Information (Agriculture)**

The USDA's Departmental Regulation 3440-2, "Control and Protection of Sensitive Security Information," defines sensitive security information as follows:

Sensitive Security Information means unclassified information of a sensitive nature, that if publicly disclosed could be expected to have a harmful impact on the security of Federal operations or assets, the public health or safety of the citizens of the United States or its residents, or the nation's long-term economic prosperity; and which describes, discusses, or reflects:

(1) The ability of any element of the critical infrastructure of the United States to resist intrusion, interference, compromise, theft, or incapacitation by either physical or computer-based attack or other similar conduct that violates Federal, State, or local law; harms interstate, international commerce of the United States; or, threatens public health or safety;

(2) Any currently viable assessment, projection, or estimate of the security vulnerability of any element of the critical infrastructure of the United States, specifically including, but not limited to vulnerability assessment, security testing, risk evaluation, risk-management planning, or risk audit;

(3) Any currently applicable operational problem or solution regarding the security of any element of the critical infrastructure of the United States, specifically including but not limited to the repair, recovery, redesign, reconstruction, relocation, insurance, and continuity of operations of any element;

(4) The following categories are provided for illustration purposes only as examples of the types of information (regardless of format) that may be categorized as SSI:

1 Physical security status of USDA laboratories, research centers, field facilities, etc., which may also contain vulnerabilities;

2 Investigative and analytical materials concerning information about physical security at USDA facilities such as the above-named facilities;

3 Information that could result in physical risk to individuals;

4 Information that could result in serious damage to critical facilities and/or infrastructures;

5 Cyber Security Information, which includes, but is not limited to:

(a) Network Drawings or Plans
(b) Program and System Security Plans
(c) Mission Critical and Sensitive Information Technology (IT) Systems and Applications
(d) Capital Planning and Investment Control Data (I-TIPS)
(e) IT Configuration Management Data and Libraries
(f) IT Restricted Space (Drawings, Plans and Equipment Specifications as well as actual space)
(g) Incident and Vulnerability Reports
(h) Risk Assessment Reports, Checklists, Trusted Facilities Manual and Security Users Guide
(i) Cyber Security Policy Guidance and Manual Chapters