3002.101 Definitions.

Adequate security means security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls.

Chief Information Officer (CIO) means the Director of the Office of the CIO.

Chief of the Contracting Office (COCO) means the individual(s) responsible for managing the contracting office(s) within a Component.

Chief Procurement Officer (CPO) means the Senior Procurement Executive (SPE).

Component means the following entities for purposes of this chapter:

(1) DHS Management (MGMT), including the Office of Procurement Operations (OPO) and the Office of Selective Acquisitions (OSA);

(2) Federal Emergency Management Agency (FEMA);

(3) Federal Law Enforcement Training Center (FLETC);

(4) Transportation Security Administration (TSA);

(5) U.S. Citizenship and Immigration Services (USCIS);

(6) U.S. Coast Guard (USCG);

(7) U.S. Customs and Border Protection (CBP);

(8) U.S. Immigration and Customs Enforcement (ICE); and

(9) U.S. Secret Service (USSS).

Contracting activity includes all the contracting offices within a Component and is the same as the term “procuring activity.”

Contracting officer means an individual authorized by virtue of position or by appointment to perform the functions assigned by the Federal Acquisition Regulation and the Homeland Security Acquisition Regulation.

Controlled unclassified information (CUI) is any information the Government creates or possesses, or an entity creates or possesses for or on behalf of the Government (other than classified information) that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls. This definition includes the following CUI categories and subcategories of information:

(1) Chemical-terrorism Vulnerability Information (CVI) as defined in 6 CFR part 27, “Chemical

Facility Anti-Terrorism Standards," and as further described in supplementary guidance issued by an authorized official of the Department of Homeland Security (including the Revised Procedural Manual "Safeguarding Information Designated as Chemical-Terrorism Vulnerability Information" dated September 2008);

(2) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (title XXII, subtitle B of the Homeland Security Act of 2002 as amended through Pub. L. 116-283), PCII's implementing regulations (6 CFR part 29), the PCII Program Procedures Manual, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security, the PCII Program Manager, or a PCII Program Manager Designee;

(3) Sensitive Security Information (SSI) as defined in 49 CFR part 1520, "Protection of Sensitive Security Information," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or designee), including Department of Homeland Security MD 11056.1, "Sensitive Security Information (SSI)" and, within the Transportation Security Administration, TSA MD 2810.1, "SSI Program";

(4) Homeland Security Agreement Information means information the Department of Homeland Security receives pursuant to an agreement with State, local, Tribal, territorial, or private sector partners that is required to be protected by that agreement. The Department receives this information in furtherance of the missions of the Department, including, but not limited to, support of the Fusion Center Initiative and activities for cyber information sharing consistent with the Cybersecurity Information Sharing Act of 2015;

(5) Homeland Security Enforcement Information means unclassified information of a sensitive nature lawfully created, possessed, or transmitted by the Department of Homeland Security in furtherance of its immigration, customs, and other civil and criminal enforcement missions, the unauthorized disclosure of which could adversely impact the mission of the Department;

(6) International Agreement Information means information the Department of Homeland Security receives that is required to be protected by an information sharing agreement or arrangement with a foreign government, an international organization of governments or any element thereof, an international or foreign public or judicial body, or an international or foreign private or non-governmental organization;

(7) Information Systems Vulnerability Information (ISVI) means:

(i) Department of Homeland Security information technology (IT) systems data revealing infrastructure used for servers, desktops, and networks; applications name, version, and release; switching, router, and gateway information; interconnections and access methods; and mission or business use/need. Examples of ISVI are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 13526 will be classified as appropriate; and/or

(ii) Information regarding developing or current technology, the release of which could hinder the objectives of the Department, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system;

(8) Operations Security Information means Department of Homeland Security information that could

be collected, analyzed, and exploited by a foreign adversary to identify intentions, capabilities, operations, and vulnerabilities that threaten operational security for the missions of the Department;

(9) Personnel Security Information means information that could result in physical risk to Department of Homeland Security personnel or other individuals whom the Department is responsible for protecting;

(10) Physical Security Information means reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities related to the protection of Federal buildings, grounds, or property. For example, threat assessments, system security plans, contingency plans, risk management plans, business impact analysis studies, and certification and accreditation documentation;

(11) Privacy Information includes both Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual; and SPII is a subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. To determine whether information is PII, DHS will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an individual. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual.

(i) Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.

(ii) Multiple pieces of information may present an increased risk of harm to the individual when combined, posing an increased risk of harm to the individual. SPII may also consist of any grouping of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(A) Truncated SSN (such as last 4 digits);

(B) Date of birth (month, day, and year);

(C) Citizenship or immigration status;

(D) Ethnic or religious affiliation;

(E) Sexual orientation;

(F) Criminal history;

(G) Medical information; and

(H) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

(iii) Other PII that may present an increased risk of harm to the individual depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individual.

Federal information means information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.

Federal information system means an information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency.

Handling means any use of controlled unclassified information, including but not limited to marking, safeguarding, transporting, disseminating, re-using, and disposing of the information.

Head of the Agency means the Secretary of the Department of Homeland Security, or, by delegation, the Under Secretary of Management.

Head of the Contracting Activity (HCA) means the official who has overall responsibility for managing the contracting activity. For DHS, the HCAs are:

(1) Director, Office of Procurement Operations (OPO);

(2) Director, Office of Selective Acquisitions (OSA);

(3) Director, Office of Acquisition Management (FEMA);

(4) Chief, Procurement Division (FLETC);

(5) Assistant Administrator for Contracting & Procurement (TSA);

(6) Chief, Office of Contracting (USCIS);

(7) Director of Contracting and Procurement (USCG);

(8) Deputy Assistant Commissioner, Office of Acquisition (CBP);

(9) Director, Office of Acquisition Management (ICE); and

(10) Chief, Procurement Operations (USSS).

Information resources means information and related resources, such as personnel, equipment, funds, and information technology.

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

(1) Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

(2) Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

(3) Availability, which means ensuring timely and reliable access to and use of information.

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Legal counsel means the Department of Homeland Security Office of the General Counsel, which includes Component offices providing legal services to the contracting organization.

Legal review means review by legal counsel.

Major system means, for DHS, that combination of elements that will function together to produce the capabilities required to fulfill a mission need, including hardware, equipment, software, or any combination thereof, but excluding construction or other improvements to real property. A DHS major system is one where the total lifecycle costs for the system are estimated to equal or exceed $300M (in constant 2009 dollars), or if the Deputy Secretary has designated a program or project as a major system. This corresponds to a DHS Level 1 or 2 capital investment acquisition.

Micro-purchase threshold is defined as in (FAR) 48 CFR 2.101, except when (HSAR) 48 CFR 3013.7003(a) applies.

Senior Procurement Executive (SPE) for the Department of Homeland Security means the individual appointed pursuant to 41 U.S.C. 1702(c). The SPE is responsible for the management direction of the procurement system of DHS, including implementation of the unique procurement policies, regulations, and standards of DHS. The DHS Chief Procurement Officer (CPO) is the SPE for DHS and is the only individual within DHS that bears the title of the CPO.

Sensitive Information, as used in this Chapter, means any information which if lost, misused, disclosed, or, without authorization, is accessed or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under 5 U.S.C. 552a (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Pub. L. 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (6 CFR part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in 49 CFR part 1520, as amended, “Policies and Procedures of Safeguarding and Control of SSI,” as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as “For Official Use Only,” which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated “sensitive” or subject to other controls, safeguards or

protections in accordance with subsequently adopted homeland security information handling procedures.

Parent topic: Subpart 3002.1—Definitions