

voluntarily submitted to the Federal Government. Title II, Subtitle B, of the Homeland Security Act is referred to herein as the CII Act of 2002. It is Department of Homeland Security (DHS) policy to encourage the voluntary submission of CII by protecting that information from unauthorized disclosure to the fullest extent permitted by law. As required by the CII Act of 2002, the procedures established herein include mechanisms regarding:

(1) The acknowledgement of receipt by a Federal agency of critical infrastructure information voluntarily submitted to the Federal Government;

(2) The maintenance of the identification of critical infrastructure information voluntarily submitted to the Federal Government for purposes of and subject to the provisions of the CII Act of 2002;

(3) The receipt, care, storage, and proper marking of the information as Protected CII;

(4) The protection and maintenance of the confidentiality of such information that permits the sharing of such information within the Federal Government and with Foreign, State, and local governments; and

(5) The issuance of notices and warnings related to the protection of critical infrastructure and protected systems in such a manner to protect from public disclosure the identity of the submitting person or entity, as well as information that is proprietary, business-sensitive, relates specifically to the submitting person or entity, and/or is not appropriately in the public domain.

(b) *Scope.* These procedures apply to all Federal agencies that receive, care for, or store CII voluntarily submitted to the Federal Government pursuant to the CII Act of 2002. In addition, these procedures apply to United States Government contractors, to Foreign, State, and local governments, and government authorities, pursuant to their express agreements.

## **§ 29.2 Definitions.**

For purposes of this part:

(a) *Critical Infrastructure* has the same definition as described in section 2 of the Homeland Security Act of 2002, and means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination thereof.

(b) *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 or information concerning:

(1) Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by 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 thereto, 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.

(c) *Critical Infrastructure Information Program or "CII Program"* means the maintenance, management, and review of these procedures and of the information provided to DHS in expectation of the protections provided by the CII Act of 2002.

(d) *Information Sharing and Analysis Organization or ISAO* means any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of:

(1) Gathering and analyzing critical infrastructure information in order to better understand security problems and interdependencies related to critical infrastructure and protected systems to ensure the availability, integrity, and reliability thereof;

(2) Communicating or disclosing critical infrastructure information to help prevent, detect, mitigate, or recover from the effects of an interference, compromise, or an incapacitation problem related to critical infrastructure or protected systems; and

(3) Voluntarily disseminating critical infrastructure information to its members, Federal, State, and local governments, or any other entities that may be of assistance in carrying out the purposes specified in paragraphs (d)(1) and (d)(2) of this section.

(e) *Local Government* has the same meaning as established in section 2 of the Homeland Security Act of 2002, and means:

(1) A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government;

(2) An Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and

(3) A rural community, unincorporated town or village, or other public entity.

(f) *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 § 29.5 of this chapter. This information maintains its protected status unless the CII Program Manager renders a final decision that the information is not Protected CII.

(g) *Protected System* means any service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of a facility of critical infrastructure and includes any physical or computer-based system, including a computer, computer system, computer or communications network, or any component hardware or element thereof, software program, processing instructions, or information or data in transmission or storage therein, irrespective of the medium of transmission or storage.

(h) *Purpose* has the meaning as described in section 214(a)(1) of the CII Act of 2002, and includes the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose.

(i) *Submission to DHS* as referenced in these procedures means any transmittal of CII from any entity to DHS. The CII may be provided to DHS either directly or indirectly via another Federal agency, which, upon receipt of the CII, will forward it to DHS.

(j) *Voluntary or Voluntarily*, when used in reference to any submission of