IM 10-07- CONTROLLED UNCLASSIFIED INFORMATION PROGRAM
APPENDIX A - DEFINITIONS

DEFINITIONS: Unless otherwise noted, these terms and their definitions are provided for best understanding of this Directive.

a. **Agency-** (also, federal agency, executive agency, executive branch agency) Any "executive agency," as defined in 5 U.S.C. 105; the United States Postal Service, and any other independent entity within the executive branch that designates or manages Controlled Unclassified Information (CUI).

b. **Agreements and arrangements-** Any vehicle that sets out specific CUI handling requirements for contractors and other information-sharing partners when the arrangement with the other party involves CUI. Agreements and arrangements include, but are not limited to, procurement contracts and interagency agreements, grants, licenses, certificates, memoranda of agreement/arrangement or understanding, and information-sharing agreements or arrangements.

c. **Alternate CUI Marking-** Any marking, authorized by PBGC's CUI Program, which is not the Standard CUI Marking.

d. **Authorized Holder-** An individual, organization, or group of users that is permitted to manage CUI, in accordance with 32 C.F.R. Part 2002. Authorized holders who create and handle CUI must be familiar with the CUI categories and CUI policies, complete all training, know how to determine what information is CUI, and how it should be managed.

e. **Controlled Environment-** Any area or space an authorized holder deems to have adequate physical or procedural controls (e.g., barriers or managed access controls) to protect CUI from unauthorized access or disclosure. For the purposes of this Directive, any PBGC-controlled space requiring a PBGC-issued PIV card for unaccompanied access is considered a "controlled environment" for the purposes of protecting CUI. For details on protecting Tax Return Information, see PBGC Directive IM 10-02, Safeguarding Tax Return Information. For details on protecting Personally Identifiable Information, see PBGC Directive IM 10-03, Protecting Personally Identifiable Information.

f. **Controlled Unclassified Information (CUI)-** Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, which a law, regulation, or government-wide policy requires or permits an agency to manage using protection or dissemination controls. CUI does not include classified information; classified information may be co-mingled with CUI and is managed and protected under classified information policies. CUI does not include information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency.

g. **Controls-** Protection or dissemination requirements that a law, regulation, or government-wide policy requires or permits agencies to use when handling CUI. The requirements may be specifically stated in the authority, or the authority may require agencies to protect the information (in which case, the agency applies the controls from E.O. 13556, this policy, and NARA's CUI Registry).

h. **CUI Categories-** Refers to the NARA designations for identifying unclassified information that a law, regulation, or government-wide policy requires or permits agencies to manage by means of protection or dissemination controls. These categories are listed in NARA's CUI Registry.

i. **CUI Executive Agent (CUI EA)-** The National Archives and Records Administration (NARA) serves as the CUI Program's Executive Agent and has delegated CUI Executive Agent responsibilities to the Director of the Information Security Oversight Office (ISOO). As the CUI EA, ISOO issues guidance to Federal agencies on handling and protecting CUI. NARA, as the CUI EA, maintains NARA's CUI Registry and the associated website, archives.gov/cui.

j. **CUI Registry-** NARA's CUI Registry serves as the government-wide central repository for all information, guidance, policy, and requirements on managing CUI, including authorized CUI categories, associated markings, handling, and decontrolling procedures. NARA's CUI Registry provides general descriptions for each category, identifies the basis for the controls, and notes any sanctions or penalties for misuse of each category.

k. **Decontrol-** Removal of protection or dissemination controls from CUI that no longer require controls. Decontrol relieves authorized holders from requirements to handle the information under PBGC's CUI Program but does not constitute authorization for public release. Decontrol may occur automatically or through agency action.

l. **Disseminate-** Dissemination occurs when authorized holders provide access, transmit, or transfer, through any means, CUI to other authorized holders, whether internal or external to the agency. Disseminating CUI to other authorized holders does not constitute decontrol of said CUI.

m. **Designation-** Determination that specific types of data or information fall into a CUI category on NARA's CUI Registry and require special handling and protection.

n. **Document-** Any tangible thing which constitutes or contains data or information, It means the original and any copies (whether different from the originals because of notes made on such copies or otherwise) of all writings of every kind and description over which an agency has authority, whether inscribed by hand or by mechanical, facsimile, electronic, magnetic, microfilm, photographic, or other means, as well as phonic or visual reproductions or oral statements, conversations, or events, and including, but not limited to: Correspondence, email, notes, reports, papers, files, manuals,

books, pamphlets, periodicals, letters, memoranda, notations, messages, telegrams, cables, facsimiles, records, studies, working papers, accounting papers, contracts, licenses, certificates, grants, agreements, computer disks, computer tapes, telephone logs, computer mail, computer printouts, worksheets, sent or received communications of any kind, teletype messages, agreements, diary entries, calendars and journals, printouts, drafts, tables, compilations, tabulations, recommendations, accounts, work papers, summaries, address books, other records and recordings or transcriptions of conferences, meetings, visits, interviews, discussions, or telephone conversations, charts, graphs, indexes, tapes, minutes, contracts, leases, invoices, records of purchase or sale correspondence, electronic or other transcription of taping of personal conversations or conferences, and any written, printed, typed, punched, taped, filmed, or graphic matter however produced or reproduced. Document also includes the file, folder, exhibits, and containers, the labels on them, and any metadata, associated with each original or copy. Document also includes voice records, film, tapes, video tapes, email, personal computer files, electronic matter, and other data compilations from which information can be obtained, including materials used in data processing.

o. **Federal information system-** An information system (a discrete set of resources organized to collect, process, maintain, use, share, disseminate, transmit, or dispose of information) used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

p. **Handling-** Any use of CUI, including, but not limited to, marking, protecting, transporting, disseminating, re-using, transmitting, and disposing of the information.

q. **Information Owner (IO)-** The PBGC official with statutory or operational authority for specified information and the responsibility for establishing the controls for a system's information generation, collection, processing, dissemination, and disposal.

r. **Information System Owner (ISO)-** The PBGC official responsible for the overall procurement, development, integration, modification, security, operation, and maintenance of an information system.

s. **Lawful Government purpose-** Any activity, mission, function, operation, or endeavor that the U.S. Government authorizes or recognizes within the scope of its legal authorities or the legal authorities of non-executive branch entities (such as state and local law enforcement). This is the standard for granting access to CUI.

t. **Limited Dissemination-** Any CUI EA-approved control on disseminating CUI.

u. **Marking-** A standard method to conspicuously identify information as CUI. The requirement provides consistent labeling and eliminates the use of ad hoc

agency specific policies, procedures, and markings to manage the information.

v. **Misuse of CUI-** Use of CUI in a manner not in accordance with E.O. 13556 *Controlled Unclassified Information*, 32 C.F.R. 2002, NARA's CUI Registry, this Directive, or the applicable laws, regulations, and government-wide policies that govern the affected information. This includes intentional unauthorized disclosures, unintentional errors in protecting or disseminating CUI, or designating or marking information as CUI when it does not qualify as CUI.

w. **National Archives and Records Administration (NARA)-** The agency that implements the executive branch-wide CUI Program and oversees federal agency actions to comply with 32 C.F.R. 2002.

x. **Non-executive branch entity-** A person or organization established, operated, and controlled by an individual or individuals acting outside the scope of official capacity as an officer, employee, or agent of the executive branch of the Federal Government. Such entities may include elements of the legislative or judicial branches of the Federal Government; State, interstate, Tribal, or local government elements; private organizations; or international individuals, including contractors and vendors. This does not include individuals or organizations that may receive CUI information pursuant to federal disclosure laws, including the Freedom of Information Act (FOIA) and the Privacy Act of 1974.

y. **Non-federal information system-** A system that contains government information but is not owned or managed by a government agency. Agencies must follow the guidelines of NIST SP 800–171 when establishing security requirements to protect CUI's confidentiality on non-federal information systems.

z. **PBGC-defined small groups-** Groups of individuals that are external to PBGC, but serve a governing, advisory, or oversight role for the agency. For this directive, examples include, but are not limited to, the Board of Directors and their representatives, the Advisory Committee, and external financial auditors.

aa. **Public release-** Occurs when an agency makes information formerly designated as CUI available to members of the public through an agency's official release process. Disseminating CUI to non-executive branch entities as authorized does not constitute public release; Releasing records containing CUI to an individual pursuant to the Privacy Act of 1974 or disclosing it in response to a FOIA request does not always constitute a public release and does not necessarily decontrol the CUI at PBGC.

bb. **Records-** All information created or received by PBGC employees and contractor employees that is evidence of PBGC's business activities and preserved, or appropriate for preservation, by PBGC. A record can be in any media format (e.g., paper, digital or photo) and should document business

activities or decisions. Also, records are defined as either temporary (having a finite retention period) or permanent (transferred to and retained permanently by NARA). Includes such items created or maintained by a government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the entity's agreement with the agency.

cc. **Safeguard-** Standards to minimize the risk of an unauthorized disclosure while allowing timely access by authorized individuals, in accordance with the agency's management and acceptance of risk. To reduce confusion with the Safeguard Program in PBGC Directive IM 10-02, this Directive will use the term "protection" and other derivations of that term when discussing "safeguarding" CUI.

dd. **Security & Privacy controls**- Any type of safeguard or countermeasure used to protect data and infrastructure important to an agency. The three main types of security controls are:
   (1) **Administrative controls**- Encompass the policies, procedures, and guidelines that promote accountability in an organization. Examples include, but are not limited to, physical access to facilities, separation of duties, data classification, and internet usage.
   (2) **Physical controls**- Use tangible obstacles to prevent or detect a potential breach of a physical perimeter. Examples include, but are not limited to, PIV cards, security guards, surveillance cameras, and locks.
   (3) **Technical controls**- Utilize technology to prevent unauthorized disclosure or compromise of data or systems or detect suspicious activity in systems. Examples include, but are not limited to, access control systems, firewalls, intrusion detection systems (IDS), and encryption measures.

ee. **Self-inspection-** An agency's internally managed review and evaluation of its activities to implement the CUI Program.

ff. **Standard CUI Marking**- The standard method to alert users and recipients of a document containing CUI. The required elements include a banner marking and a designation indicator.

gg. **Unauthorized disclosure (UD)-** Unauthorized disclosure occurs when an authorized holder of CUI intentionally or unintentionally discloses CUI without a lawful Government purpose, in violation of restrictions imposed by safeguarding or dissemination controls, or contrary to limited dissemination controls.