Subpart AA. Safeguarding

Section 1.0 – General Policy

(a) The executive branch strives to share information to the widest extent possible. In all cases, care should be taken not to place undue burdens on the recipients of CUI. Reasonable safeguarding measures are required for all CUI to protect it from unauthorized or inadvertent disclosure. Measures to protect data confidentiality shall be implemented to manage the risks associated with the processing, storage, transmission, and destruction of CUI. The CUI Executive Agent shall identify reasonable safeguarding measures in detail in the CUI Registry.

(1) At the "Controlled" level: The purpose is to enable rapid, efficient, and affordable sharing of CUI. Required safeguards are limited to measures that are believed to be practicable for authorized recipients of CUI.

(2) At the "Controlled Enhanced" level: More stringent safeguarding measures are required due to the particularly sensitive nature of the information. Safeguarding this CUI is sufficiently critical to justify the imposition of potentially significant operational inefficiencies, delays, or financial burdens.

(b) The Controlled level shall be the standard, baseline safeguarding level. Providers of CUI shall require safeguards at the "Controlled Enhanced" level only when the necessity for doing so is clear. Agency heads shall limit the designation of information as "Controlled Enhanced."

(c) The originator of CUI shall not impose additional safeguards beyond those published in the CUI Registry upon a recipient outside of the originating Agency.

(d) Authorized recipients outside of the executive branch shall safeguard CUI in accordance with this Directive. Entities outside of the executive branch may adopt alternative equivalent measures, using risk management principles.

Section 2.0 – Waivers for Exigent Situations

(a) Agency heads, or their Designees, may authorize temporary waivers to the safeguarding requirements within their organization in emergency situations. At the resolution of the emergency situation, the Agency shall reinstitute the safeguarding requirements.

(b) Agency heads, or their Designees, may authorize temporary waivers to the safeguarding requirements for personnel conducting field operations where the operating environment precludes their ready access to the means to adhere to the safeguarding requirements.

(c) Agency heads, or their Designees, shall report waivers in writing to the CUI Executive Agent promptly.

(d) The CUI Executive Agent shall publish notice of waivers in the CUI Registry.

(e) The CUI Executive Agent may rescind safeguarding waivers for cause.

Section 3.0 – Controls in Use

(a) Agency heads are responsible for implementing a system of control measures, in accordance with applicable guidance published in the CUI Registry, for CUI in their possession or control. These control measures shall be designed to reduce the risk that CUI can be exposed to or directly observed by an unintended recipient or that conversations regarding CUI can be overheard by an unintended recipient.

(b) All CUI shall be marked as per Subpart XX of this Directive.

(c) CUI may be reproduced without the permission of the originator as required to carry out official duties, provided that the reproduced material is marked in the same manner as the original material. Printing of copies from electronic media shall be considered reproduction.

For future development: policy for when CUI is incorporated, paraphrased, restated, or generated in new form into a new document to be developed with the marking section, specifically portion marking.

(d) CUI may be processed only on information systems which employ state-of-practice computer security measures published in the CUI Registry.

For CUI Registry: FISMA standards for executive branch.

(e) CUI shall not be processed on devices where physical access to the device is available to the general public.

For CUI Registry: This applies to use of computers in libraries, internet cafes, hotel business centers, etc.

(f) *Personally owned electronic devices.* CUI shall not be processed on personally owned electronic devices unless the Agency head or his/her Designee has a process in place to adequately protect CUI on the device. The process must require control measures on the device to be approved by an Agency Information Security official. The following safeguards also apply:

(1) At the Controlled Level: the agency process shall limit the saving of CUI on personally owned electronic devices based on risk management principles.

(2) At the Controlled Enhanced Level: the agency process shall prohibit individuals from saving CUI on personally owned electronic devices.

(g) When CUI is processed on mobile devices outside of a Controlled Environment, authentication procedures are required according to the standards published in the CUI registry.

> For CUI Registry: Use a "time-out" function requiring user re-authentication after 30 minutes inactivity. E-authentication identity proofing and authentication at level 2 or higher is required.

SECTION 4.0 – Storage

(a) *General*. When CUI is not under the direct control of an individual authorized to access it, the CUI shall be protected by:

(1) At the Controlled Level: For each access path, one physical or electronic barrier that shall deter access from those not authorized to access the CUI.

(2) At the Controlled Enhanced level: For each access path, two physical or electronic barriers that shall deter access from those not authorized to access the CUI. A physical barrier and an electronic barrier can be combined to satisfy the two barrier requirement.

(b) *Physical barriers.* Examples of physical barriers include, but are not limited to, an area protected by a human guard, a key card system or lock, and locked receptacles (e.g., file drawer, desk drawer). Specific standards shall be published in the CUI Registry.

(c) *Electronic barriers*. An electronic barrier shall control access in a way that requires authentication of the user or provides encryption at the standards published in the CUI registry. A controlled interface that meets standards set forth by the CUI Executive Agent shall be used on an Internet facing path. This controlled interface shall constitute one barrier on the Internet facing path.

> For CUI Registry: In order for authentication to qualify as a storage barrier, for either level, the standard shall be at e-authentication level 2 or higher which requires a username and password. In order for encryption to qualify as a storage barrier at the Controlled Level, the standard would be FIPS 140-2 Security Level 1. In order for encryption to qualify as a storage barrier at the Controlled Enhanced Level, the standard would be FIPS 140-2 Security Level 2.

(d) Knowledge of the password or access to the key necessary to penetrate the barrier shall be limited based on operational requirements to the personnel who are authorized to access the CUI.

(e) *Storing in the open.* Agency heads may allow unattended storage openly on desks or tables, or in unlocked containers within a Controlled Environment in which there exists adequate

physical barriers and access controls as indicated in section (b) above, sufficient to deter unauthorized entry.

(f) *Removable electronic media.* All CUI on removable electronic media shall be protected by an electronic barrier of encryption at the standards published in the CUI Registry.

For CUI Registry: Encryption at the FIPS 140-2 Security Level 1 for Controlled and at FIPS 140-2 Security Level 2 for Controlled Enhanced. Controlled Enhanced CUI will still need an additional barrier.

SECTION 5.0 – Transmission

(a) CUI shall be transmitted and received in a manner that reduces the risk of inadvertent or unauthorized disclosure and that provides a method which assures timely delivery to the intended recipient. While transmitting or receiving CUI, the CUI Dissemination policy shall be followed.

(b) The sender is responsible for compliance with the safeguards established by the CUI Executive Agent when sending CUI. The sender is not responsible for ensuring that the recipient properly safeguards the CUI. The recipient has the responsibility of safeguarding received material in accordance with the CUI Memorandum, this Directive, and guidance published in the CUI Registry.

(c) Agency heads shall establish internal procedures, based on the CUI Memorandum, this Directive, and guidance published in the CUI Registry, that are designed so that CUI is received in a manner that reduces the risk of inadvertent or unauthorized disclosure.

(d) In addition to the general policy set forth in subsections (a) through (c), certain methods of transmission require additional safeguards in order to protect CUI from unauthorized or inadvertent disclosure. These additional transmission safeguards are set forth in Sections 5.1 through 5.3.

Section 5.1 - Physical transmission

(a) While in transit outside of a Controlled Environment and not under the direct control of a person authorized to access the CUI, unencrypted CUI shall:

(1) At the Controlled Level: be enclosed in a single layer of either a sealed, opaque wrapping or a sealed or locked opaque container.

(2) At the Controlled Enhanced level:

(i) be enclosed in two layers of sealed opaque wrappings or sealed or locked opaque containers, both of which provide reasonable evidence of tampering and which conceal the contents. The outer wrapping or container shall not contain an

indication that CUI material is enclosed. The inner wrapping or container must be marked to indicate the designation of the CUI contained therein.

(ii) be transmitted only by express mail, registered mail, certified mail or first class/priority mail with a prohibition against forwarding if transmitted by U.S. Postal Service. A signature receipt is required.

(iii) be transmitted by courier only if the courier utilizes receipts upon pickup and delivery.

(iv) be transmitted by commercial delivery service only if the commercial delivery service provides automated in-transit tracking of the CUI. The signature waiver block shall not be executed.

(b) While in transit outside of a Controlled Environment and not under the direct control of a person authorized to access the CUI, CUI encrypted at the standard published in the CUI registry:

(1) At the Controlled level: shall not require a wrapping or container.

(2) At the Controlled Enhanced level: shall require a single layer of either a sealed, opaque wrapping or a sealed or locked opaque container.

Section 5.2 - Voice and fax transmission

(a) Fax transmission of CUI is permitted:

(1) At the Controlled Level: when the receiving fax machine is within a Controlled Environment or the sender has confirmed that someone authorized to receive the CUI will attend the fax machine until the transmittal is complete.

(2) At the Controlled Enhanced level: when the sender has confirmed that someone authorized to receive the CUI will attend the fax machine until the transmittal is complete. The recipient shall promptly acknowledge receipt of the facsimile.

(b) *Voice transmission*:

(1) At the Controlled Level: Broadcast radio transmission over unencrypted channels shall be avoided when operationally feasible.

(2) At the Controlled Enhanced level: Voice telephone transmission and reception should avoid the use of cordless or mobile phones when operationally feasible. Broadcast radio transmission over unencrypted channels is prohibited.

Section 5.3 - Electronic transmission

(a) If CUI is transmitted on a stand-alone system or a system that is connected to others in a Controlled Environment but has no transmission path over a public telecommunications network, no further safeguards are required for electronic transmission.

(b) When CUI is transmitted on an information processing system with physical or logical connections outside of a Controlled Environment, the following safeguards apply:

(1) CUI shall be transmitted using technology/processes that encrypt the data or secure the transmission path. The technology/processes shall meet the standards published in the CUI registry.

(2) CUI shall only be accessed through a system that authenticates users or systems. The authentication shall meet the standards published in the CUI registry.

(3) The administrator of a transmitting system shall implement procedures to provide for transmission security of information available on the system.

For CUI Registry:
Encryption shall be implemented in accordance with FIPS 140-2, Security Level 1 which provides basic encryption. A Virtual Private Network (VPN) and secured sockets (https) are examples of secured paths. Authentication standard: e-authentication level 2 or higher which requires a username and password. A LAN is an example of a system that is connected to others in a Controlled Environment but has no access/transmission paths over public telecommunications network.

(c) Transmission via Website: In addition to the requirements specified in subsection 5.3 (b) (1)-(3) above,

(1) CUI may not be posted to websites that are publicly available or that limit access only by domain/IP restriction.

(2) At the Controlled Level: CUI shall be posted only to websites that meet the standards published in the CUI Registry. Access control may be provided at the network level (e.g., intranet) where the Agency head or his/her Designee determines is appropriate.

(3) At the Controlled Enhanced level: CUI shall be posted only to websites that require two-factor authentication for access where one of the factors is provided by a device separate from the device gaining access.

(4) Specified Dissemination: CUI shall be posted only to websites that limit dissemination to those with authorized access in accordance to dissemination limitations. Access control measures shall meet the standard published in the CUI registry.

For CUI Registry: Access control: System shall have a means of vetting users equivalent to e-authentication identity proofing level 2 and allow the equivalent of e-authentication level 2: user identification/password, user certificates, or other technical means that preclude unauthorized access. Use a "time-out" function requiring user re-authentication after 30 minutes inactivity. Protection measures: secure sockets or equivalent technology.

SECTION 6.0 – Destruction

(a) *General.* CUI shall be destroyed in a manner that precludes routine recognition or reconstruction of the information.

(b) *Physical.* The methods approved to destroy CUI are burning, cross-cut shredding, wet-pulping, melting, mutilation, chemical decomposition, or pulverizing.

(c) *Electronic.* CUI in electronic form shall be deleted and also removed from any desktop trash or recycling file. When any electronic device that has stored CUI is sold, transferred, or reassigned to a person not authorized access to the CUI, it shall be sanitized at the standard set by the CUI Executive Agent.

For CUI Registry: Standards from NIST SP 800-88 – "clear" for Controlled and "purge" for Controlled Enhanced.

(These sections should be in directive, but not in Safeguarding Part)

Section VV – Definitions *[still in development]*

Agency: When used in this directive, has the same meaning as "Departments and Agencies" as defined in the President's May 9, 2008 memorandum regarding Designation and Sharing of Controlled Unclassified Information.

Controlled Environment: a physical location where access is restricted or where procedural measures are in place to limit CUI access to individuals authorized at a particular CUI safeguarding and dissemination level.
.

CUI Memorandum: the President's May 9, 2008 memorandum regarding Designation and Sharing of Controlled Unclassified Information.

External storage device: a data storage device that is not permanently installed in a personal computing device, such as a memory card, thumb or USB 'flash' drive, DVD, CD ROM, diskette, or comparable device.

Mobile device: removable and/or portable computing device such as a laptop computer, a personal digital assistant, or a smart phone.

Removable electronic media: Includes both mobile devices and external storage devices

State-of-practice: the conditions most generally existing or common at a given time.

Website: the collection of information, Internet media, services, supporting technology and system available at a Uniform Resource Locator (URL) (i.e., a Web address that begins with the protocol indicator of ftp, http, or https). Includes Web portals, Really Simple Syndication (RSS), Web logs (BLOGs), video and audio streaming, file downloading and other Internet media and services initially accessed via a URL.

Section WW - Establishment of a CUI Program *[still in development]*

(a) Agency heads shall establish a CUI Program to safeguard CUI, appropriate to the environment in which the access occurs and the nature and volume of the information. The Program shall include technical, physical, and procedural measures.

(b) As part of an agency's CUI Program, the agency head shall include procedures for internal reviews and inspections.

(c) The agency head shall refer any matter pertaining to the implementation of this Directive that cannot be resolved to the CUI Executive Agent for resolution.

Section YY – Loss, violation, or unauthorized disclosure *[still in development]*

(a) *Duty to report.* Persons authorized to access CUI shall promptly report any suspected or actual violation of safeguarding procedures, the loss or misplacement of CUI and any suspected or actual unauthorized or inadvertent disclosure of CUI to the Agency Head or an official designated for that purpose.

(b) *Inquiry/investigation.* Agency heads shall establish appropriate procedures to conduct an inquiry/ investigation of a suspected or actual violation of safeguarding procedures, the loss or misplacement of CUI, and any suspected or actual unauthorized or inadvertent disclosure of CUI in order to implement appropriate corrective actions.