Background on the Controlled Unclassified Information Framework

May 20, 2008

To Accompany the Presidential Memorandum:

Designation and Sharing of Controlled Unclassified Information (CUI)

(Released May 09, 2008)

The global nature of the threats our Nation faces today requires that: (1) our Nation's entire network of defenders be able to share information more rapidly and confidently so that those who must act have the information they need, and (2) the government protect sensitive information and information privacy rights and other legal rights of Americans. The lack of a uniform government-wide control framework for Sensitive But Unclassified (SBU) information severely impedes these dual imperatives. Such a framework k for SBU information is an essential attribute of the Information Sharing Environment (ISE), the creation of which has been mandated by the Congress and the President.

Accordingly, on May 09, 2008, the President released the Memorandum for the Heads of Departments and Agencies on the Designation and Sharing of Controlled Unclassified Information. The Presidential Memorandum "(a) adopts, defines, and institutes "Controlled Unclassified Information" (CUI) as the single, categorical designation henceforth throughout the executive branch for all information within the scope of that definition, which includes most information heretofore referred to as "Sensitive But Unclassified" (SBU) in the Information Sharing Environment (ISE), and (b) establishes a corresponding new CUI Framework for designating, marking, safeguarding, and disseminating information designated as CUI. This CUI Framework will streamline the sharing of unclassified terrorism-related information across the United States Government, thereby improving the daily operations of the agencies within the ISE that are responsible for protecting the homeland."

The following document reflects judgments of executive departments and agency experts within the ISE, and responds to direction provided by the 9/11 Commission, Congress, and the President. It accompanies the Presidential Memorandum (May 09, 2008) to provide Heads of Executive Departments and Agencies with the background on the development and details of the CUI Framework.

I. The CUI Framework

SBU information is shared today according to an ungoverned and diverse body of policies and practices that confuse both its producers and users. Current sharing practices not only impede the timeliness, accuracy, and ready flow of terrorism information that should be shared, but often fail to control the flow of information that should not be shared. Because each department and agency within the Executive Branch largely establishes its own access controls, an individual who has access to controlled information in one agency may be denied access to that same information in another. Moreover, an organization that receives controlled information from several different Federal agencies often cannot be sure which controls should be applied to which markings from another agency. These diverse practices greatly increase the likelihood of erroneous handling and dissemination of information.

On December 16, 2005, the President issued a Memorandum to the Heads of Executive Departments and Agencies on the *Guidelines and Requirements in Support of the Information Sharing Environment.* This memorandum provided direction to Federal departments and agencies on the standardization of procedures for designating, marking and handling SBU information. Specifically, Presidential Guideline 3 instructed that, "To promote and enhance the effective and efficient acquisition, access, retention, production, use, management, and sharing of Sensitive But Unclassified (SBU) information, including homeland security information, law enforcement information, and terrorism information,[1] procedures and standards for designating, marking, and handling SBU information (collectively "SBU procedures") must be standardized across the Federal government."

An interagency SBU Working Group, co-chaired by the Departments of Justice (DOJ) and Homeland Security (DHS), initiated efforts to formulate the required Presidential Guideline 3 recommendations.

---

[1] Pursuant to the ISE Implementation Plan, and consistent with Presidential Guidelines 2 and 3, the ISE will facilitate the sharing of "terrorism information," as defined in IRTPA section 1016(a)(4), as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information": (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)); and (2) law enforcement information relating to terrorism or the security of our homeland. Such additional information includes intelligence information.

Those efforts provided a solid foundation for completing the subsequent work that was necessary to fully address the elements required by Guideline 3.

Guideline 3 recommendations were subsequently completed under the auspices of a Guideline 3 Coordination Committee (CC), known as the SBU CC. The SBU CC, chaired by the Program Manager for the Information Sharing Environment (PM-ISE) with Homeland Security Council (HSC) oversight, was composed of representatives from the Departments of State (DOS), Defense (DoD), Justice (DOJ), Transportation (DOT), Energy (DOE), and Homeland Security (DHS); the Federal Bureau of Investigation; the Office of the Director of National Intelligence (ODNI); the National Security Council; and the Office of Management and Budget (OMB). These efforts involved consultation, as appropriate, with experts from other affected entities, including the National Archives and Records Administration (NARA), the Information Security Oversight Office, the Controlled Access Program Coordination Office, the Information Sharing Council, the Global Justice Information Sharing Initiative, and other State, local, and tribal partners and the private sector.

The final *Presidential Guideline 3 Report: Standardize Procedures for Sensitive But Unclassified (SBU)* Information recommended to the President the new Controlled Unclassified Information (CUI) Framework for rationalizing, standardizing, and simplifying procedures for information in the ISE.

> ***Rationalization*** means establishing a framework that is based on a set of basic principles that are easily understood by all users. A rationalized framework should improve confidence among users and the American public that information is being shared and protected in a way that properly controls only information that should be controlled and protects the privacy and other legal rights of Americans.
>
> ***Standardization*** means structuring a framework in which all participants are governed by the same definitions and practices that must be uniformly applied by all users. The objective is to end uncertainty and confusion about how others using the framework will handle and disseminate CUI information. Accomplishing this objective is critical to our State, local, tribal, private sector, and foreign partners, which require a standardized system, especially for use by first responders. Standardization helps achieve the vision for the ISE as mandated by Congress: "*a trusted partnership between all levels of government.*"
>
> ***Simplification*** means operating a framework that has adequate, but carefully limited, numbers and types of markings, safeguards, and dissemination standards for CUI information. Such a simplified Framework should facilitate Federal, State, local, and tribal governments sharing across jurisdictions; facilitate the training of users; and reduce mistakes and confusion.

In Guideline 3, the President directed that standardization recommendations be submitted in the first instance for "homeland security information, law enforcement information, and terrorism information." The President further directed that standardization recommendations be submitted in the next instance for "all types of information not addressed" in the first instance (i.e., SBU information sharing within the ISE other than homeland security information, law enforcement information, and terrorism information). Accordingly, efforts to prepare the recommendations for the President focused on developing standardization recommendations for homeland security information, law enforcement information, and terrorism information, as those terms are defined in the ISE Implementation Plan, and then for all other ISE SBU information. The report to the President recognized that the President's Guideline 3 does not encompass non-ISE SBU information; however, in developing the standardization recommendations, the report also recognized that the scope of ISE information may be expanded at a future date to include other SBU information. Since it is highly unlikely that Federal departments and agencies will find it cost-effective to maintain both a new CUI Framework for ISE information and the old SBU Framework for non-ISE information, the CUI Framework was structured so that it may be applied to broad processes and technologies for handling all types of SBU information.

II. Current SBU Environment

Across the Federal government there are more than 107 unique markings and over 130 different labeling

or handling processes and procedures for SBU information. These processes and procedures fall into three categories: (1) those that were created by statute or implement a statute; (2) those that were created by a Federal regulation based on a notice-and-comment rulemaking process; and (3) those that are based on individual department and agency directives, orders, or other administrative documents. Of the existing department and agency policies for marking and handling, the great majority have been derived from documents that address specific department or agency missions and/or the general nature and use of protected data without attention to the overall Federal environment of SBU information sharing and protection. Hence, the current processes for marking, safeguarding, and dissemination of SBU information are inconsistent and confusing across Federal departments and agencies.

Certain statutes govern how the Federal government, as well as State, local, and tribal governments and the private sector, must recognize, safeguard, and use SBU information. In addition, the management of information in the Federal government's possession is governed by laws such as the Freedom of Information Act (FOIA), the Privacy Act of 1974, and the Federal Information Security Management Act, as well as Executive Order 12333.2 The proposed standardization of SBU procedures through a new CUI Framework has taken these statutes into account, recognizing that nothing in the standardization should impact the legal obligations imposed by these statutes.

III. CUI Framework Policy

The policies set forth in the Presidential Memorandum for the designation, marking, safeguarding, and disseminating of CUI are mandatory for all CUI originated by the Executive Branch of government and shared within the ISE, regardless of the medium used for its display, storage, or transmittal. The following sections provide additional details and background on the CUI Framework, as developed by the interagency coordinating committee and approved by the President.

It is important to note that the Presidential Memorandum also encourages the adoption of the CUI Framework by State, local, tribal, and private sector entities. Frequent consultations with individuals and organizations from these entities during the development of this Framework suggest that there is some support for moving in the direction of a common—or mostly common—CUI Framework. As necessary, departments and agencies may agree with foreign partners to ensure they protect shared CUI in "a like manner," similar to what is now done for sharing classified information. Presidential Guideline 4 activities address foreign government sharing, including sharing of CUI.[3] Additionally, sharing CUI with the private sector will most likely require some change to an agency's contractual policy, which may include mandating the use of the CUI Framework. Continued coordination with non-Federal entities should be an objective of the CUI Governance Structure.

The term Controlled Unclassified Information or CUI is a *categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. Henceforth, the designation CUI replaces "Sensitive But Unclassified" (SBU).*

The change in nomenclature from *SBU* to *CUI* reflects the notion that "legacy terminology" (i.e., SBU terminology) should not be used in the new CUI Framework. Transitioning to new terminology will avoid confusion with markings that will no longer be authorized and will emphasize the need for a new and strengthened attitude in favor of sharing.

CUI Designation

1. Information shall be designated as CUI if:
   a. a statute so requires or authorizes; or

---

[2] This does not affect existing statutory requirements for records management.
[3] The full text of Presidential Guideline 4 can be found at:
http://www.ise.gov/docs/guideline%204%20%20sharing%20with% 20foreign%20partners.pdf.

b. the head of the originating department or agency, through regulations, directives, or other specific guidance to the agency, determines that the information is CUI. Such determination should be based on mission requirements, business prudence, legal privilege, the protection of personal or commercial rights, or safety or security. Such department or agency directives, regulations, or guidance shall be provided to the CUI Executive Agent for his review.

2. Notwithstanding the above, information shall not be designated as CUI:

   a. to: (1) conceal violations of law, inefficiency, or administrative error; (2) prevent embarrassment to the U.S. Government, any U.S. official, organization, or agency; (3) improperly or unlawfully interfere with competition; or (4) prevent or delay the release of information that does not require such protection;

   b. if it is required by statute or Executive Order to be made available to the public; or

   c. if it has been released to the public under proper authority.

As a matter of policy, the CUI Framework includes the following:

1. All CUI markings in the ISE shall conform to the CUI Framework.

2. Wherever possible, it is expected that departments and agencies will re-mark archived or legacy material when it is migrated into the ISE. However, if the cost of re-marking archived or legacy documents is excessive, departments and agencies should advise recipients that CUI replaces all SBU markings. Newly-created CUI shared within the ISE shall not carry any legacy markings unless the originator is outside the Federal government (State, local, or tribal entities or foreign partners), in which case a legacy marking shall be retained unless the originator authorizes its removal. Non-Federal entities are strongly encouraged to use the new CUI markings. If a non-Federal entity requests that a legacy marking be included on its document, the receiving Federal agency shall do so. However, the Federal agency shall also apply the appropriate standard CUI marking, per this Framework.

3. The marking may inform but will not be determinative of public disclosure and release decisions, such as those made pursuant to FOIA. The CUI Framework will have no impact on the processes mandated by FOIA; information made public as the result of a FOIA process will thereafter be ineligible for CUI status.

4. The originating agency should use portion marking for material that contains both CUI and non-CUI information or that contains multiple levels of CUI.

5. The CUI Framework shall be incorporated into ISE-related information technology (IT) projects under development or developed in the future and be reflected in the development of plans for new information technologies. ISE-related IT systems shall be developed and upgraded to protect CUI information as appropriate and in accordance with the data protection requirements of the CUI Framework and applicable privacy and statutory requirements.

6. The CUI marking shall be used regardless of the medium in which the information appears. Oral communications should be prefaced with a statement describing the controls when necessary to ensure recipients are aware of the information's status.

7. Departments or agencies shall not impose safeguarding requirements or dissemination controls on information in the ISE that is neither classified nor CUI.[4]

8. The length of time during which particular information requires CUI status varies from a few hours (e.g., embargoed press releases) to many decades (e.g., some privacy information or proprietary information). There are numerous Federal statutes and regulations that bear upon the duration of CUI status for particular kinds of information. Accordingly, a government-wide policy prescribing the CUI life cycle is inappropriate. However, NARA, as the CUI Executive Agent, is well-suited to

[4] This, however, does not imply that information not designated CUI is approved for public release unless an affirmative determination has been made through appropriate department and agency procedures.

provide expertise on this issue. In the interim, the FOIA process will provide a straightforward way for anyone to seek public release of CUI and ensure that all CUI for which there is a demand will be carefully reviewed for release.

CUI Marking

Marking material as CUI signals that it contains sensitive information and that safeguarding and dissemination controls apply.

All CUI will carry one of three markings:

Controlled with Standard Dissemination: Information is subject to safeguarding measures that reduce the risks of unauthorized or inadvertent disclosure. Dissemination is permitted to the extent that it is reasonably believed that it would further the execution of a lawful or official purpose.

Controlled with Specified Dissemination: Information is subject to safeguarding measures that reduce the risks of unauthorized or inadvertent disclosure. Material contains additional instructions on what dissemination is permitted.

Controlled Enhanced with Specified Dissemination: Information is subject to enhanced safeguarding measures more stringent than those normally required since inadvertent or unauthorized disclosure would create a risk of substantial harm. Material contains additional instructions on what dissemination is permitted.

The decision to use "Controlled" as the CUI signifier was a direct result of department and agency discussion with State and local partners, who sought a clear marking to simplify their work.

All CUI will be marked in a clear and conspicuous manner. CUI markings shall conform to statutory or regulatory placement requirements, if any. If a recipient receives CUI that is not marked, he or she shall mark the information appropriately and inform the sender that the information should be marked.

CUI Safeguarding

The marking "*Controlled*" means that the information is subject to standard CUI safeguarding procedures to reduce the risks of unauthorized or inadvertent disclosure.

The marking "*Controlled Enhanced*" means enhanced safeguarding is required since inadvertent or unauthorized disclosure would create risk of substantial harm.

Reasonable safeguarding measures are required for all CUI information to protect it from unauthorized or inadvertent release. These measures to protect data confidentiality shall be implemented to manage the risks associated with the communication, processing, storage, and lifecycle of CUI. Defined safeguarding standards will be published in a CUI Framework Standards Registry (the CUI Registry) that the CUI Executive Agent maintains. No recipient of CUI, shared within the ISE, may be required by the originator to implement additional safeguards beyond those published in the CUI Registry. There are current SBU regimes that have criminal or civil penalties defined by statute; nothing in this Framework changes those currently applicable statutes. Recipients of CUI have a duty to report any unauthorized or inadvertent disclosures to the designating agency. The guiding principle for these standards is risk management. In all cases, care should be taken not to place undue burdens on the recipients of CUI information; in particular, providers of CUI shall require safeguards at the "Controlled Enhanced" level only when the necessity for doing so is clear.

The Framework establishes safeguarding standards that should be required, focusing on drawing the lines between protective measures that are considered essential and areas where risks should be accepted in order to enable effective and efficient operations. As CUI Executive Agent, NARA will maintain detailed requirements that may be modified over time to account for changes in widely available information technologies. Moreover, NARA will ensure there is sufficient flexibility in the detailed standards to allow alternative approaches to equally protect controlled information.

The safeguarding standards mandated by this Framework are the requirements that recipients of shared CUI must follow. Federal departments and agencies should establish and follow additional Federal

standards, such as information security standards, as required in the course of implementing statutes and Federal policies through CUI governance processes and NIST standards.

The Federal government recognizes that it may take some time for State, tribal, local, and private sector recipients of CUI to implement all of these safeguarding requirements, particularly the requirements for encryption of CUI during electronic storage and transmission. Because of the importance of prompt sharing of CUI, a phased approach for implementation, which provides the necessary flexibility for transitioning to the new CUI Framework, is recommended. During this phased approach, Federal departments and agencies should be willing to share CUI with State, tribal, local, and private sector partners that have not fully implemented the encryption aspects of the safeguarding requirements.

The proposed requirements for both levels are detailed below.

Topic	Controlled	Controlled Enhanced
Overall Definition	"Controlled" safeguards are defined as measures that recipients of CUI are required to take to reduce the risks of unauthorized or inadvertent disclosure (e.g., as a result of carelessness, theft, or electronic intrusion).	"Controlled Enhanced" safeguards are defined as measures more stringent than those normally required since inadvertent or unauthorized disclosure would create a risk of substantial harm.
Introduction	Most CUI will be marked "Controlled," to indicate that (a) the information is sensitive, and care shall be taken to avoid inadvertent or unauthorized disclosure, and (b) in the interest of enabling rapid, efficient, and affordable sharing of CUI within the ISE, required safeguards are limited to measures that are believed to be practicable in the near term for all authorized recipients of CUI. Accordingly, senior officials may authorize occasional exceptions to the requirements attached to "Controlled" CUI based on operational necessity or unusual urgency.	Some CUI will be marked "Controlled enhanced," to indicate that (a) the information is particularly sensitive, and more stringent safeguarding measures are required, and (b) safeguarding this particular CUI is sufficiently critical to justify the imposition of significant operational inefficiencies, delays, or financial burdens on some authorized recipients.
Precautions/ Handling	Possessors of CUI shall mark all CUI as such; take care that state-of-practice computer security measures are used to protect from intrusions in computers and computer networks that process CUI; and refrain from processing CUI on computers with public or open access to which access is not controlled. In addition, the safeguarding steps shall include careful operational practices designed to minimize the risk that CUI on a computer screen or on paper can be read by an unauthorized person, or that conversations regarding CUI can be overheard. CUI may be reproduced to the minimum extent necessary to carry out official duties.	This marking indicates that the following safeguards are required in addition to the safeguards for "Controlled" CUI: External markings on all documents or media; conduct periodic internal reviews of handling practices; and periodic inspections of the implementation of established policy.

Topic	Controlled	Controlled Enhanced
Storage	When CUI is not under the direct control of an individual authorized to access it, it shall be protected from unauthorized scrutiny or theft by at least one physical or electronic barrier, such as a lock or a password. The key or password necessary to penetrate the barrier shall not be available to anyone not authorized to access the CUI the barrier protects. Electronic media storing CUI must be protected by encryption.	This marking indicates that the following safeguards are required in addition to the safeguards for "Controlled" CUI: A second physical or electronic barrier.
Destruction	When destroyed or discarded, CUI shall be destroyed in a manner that prevents routine recognition or reconstruction. 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 for access to the CUI, it shall be sanitized (e.g., by erasure and overwriting) to ensure that the CUI can no longer be accessed or recovered.	This marking indicates that the following safeguards are required in addition to the safeguards for "Controlled" CUI: To ensure that such information in electronic form is destroyed prior to making the storage medium available to those not authorized to access the information, it may not be stored on a non-Federal computer, device, or medium unless the owner agrees in writing that the computer, device, or medium will be subject to all the controls listed here, including sanitization prior to its sale or reassignment to a user not authorized to access this information and whenever the owner ceases to be authorized to access this information.
Transmission	*[Physical media or devices containing CUI]* While in transit outside a controlled environment, unencrypted CUI shall be in an opaque wrapping or container, and this wrapping or container shall be either sealed or locked when it is not under the direct control of a person authorized to access the CUI. *[Electronic Transmission]* Email, text messages, and similar	*[Physical media or devices containing CUI]* This marking indicates that the following safeguards are required in addition safeguards for "Controlled" CUI: U.S. Postal Service transmission shall be by registered mail or by first class/priority mail with a prohibition against forwarding; all other couriers shall utilize receipts upon pickup and delivery; and two layers of sealed/locked opaque wrappings or containers shall be used, with no indication on the outer wrapping or container that CUI material is enclosed. Electronic material that is encrypted does not require opaque/locked wrappings/containers. *[Electronic Transmission]* This marking indicates that the following

Topic	Controlled	Controlled Enhanced
	communications of CUI should be transmitted using technology/processes such as closed networks, virtual private networks (VPN), and PKI. Information must be encrypted during transit.	safeguards are required in addition to the safeguards for "Controlled" CUI: No additional safeguards
	[Voice and Fax Transmission] Voice and fax transmission of CUI is permitted only when the sender has reasonable assurance that only persons authorized to receive the CUI will have access to the information. Easily monitored voice transmission (e.g., use of police radios on normal frequencies) is prohibited.	*[Voice and Fax Transmission]* This marking indicates that the following safeguards are required in addition to the safeguards for "Controlled" CUI: Fax transmission of CUI is permitted only when the sender has confirmed that only persons authorized to receive the CUI will have access to the received fax; voice telephone transmission and reception should avoid the use of cordless or mobile phones when operationally feasible; and to share information with authorized foreign governments, use of their telephone systems is permitted.
	[*Transmission via a Website*] CUI may not be posted on a web site which is publicly available or has access limited only by domain/IP restriction. It may be posted to Websites which control access by user identification/password, user certificates, or other technical means that preclude unauthorized access, and which provide protection via use of secure sockets or other equivalent technologies. Access control may be provided at the network level (e.g., intranet) where appropriate. CUI with "Specified Dissemination" may be posted only to Websites that limit dissemination to those authorized access in accordance with the dissemination limitations.	*[Transmission via a Website]* This marking indicates that the following safeguard is desirable, but not mandatory in addition to the safeguards for "Controlled" CUI: "Controlled enhanced" CUI may be posted only to Websites that require two-factor authentication for access.

CUI Dissemination

The marking of "*Standard Dissemination*" means: (1) dissemination is authorized to the extent that it is reasonably believed that it would further the execution of a lawful or official mission or purpose, provided that the individual disseminating this information does so within the scope of his/her assigned duties; and (2) the originating department or agency retains control of this information with regard to authorized release to the public or media and is providing this information with a clear expectation that confidentiality will be preserved. Any release of CUI to the public should be determined by relevant departments and agencies as part of their existing procedures.

Material marked "*Specified Dissemination*" must contain additional instructions on what dissemination is permitted. Departments and agencies that originated the information will determine whether such information shall be marked as "Specified Dissemination." These instructions will appear at the beginning of the document, and all electronic documents containing metadata tags shall include a tag instruction. Any Specified Dissemination instructions:

1. Shall state objective rather than subjective criteria, and be based on the subject matter contained in the controlled material.
2. Shall be defined by department and agency heads, with CUI Executive Agent approval, and listed in the CUI Registry maintained by the CUI Executive Agent. This approach will achieve standardization and avoid inconsistencies in definitions among departments and agencies and will allow recipients to readily look up the definitions. A registered instruction may contain a blank to be filled in. Examples of possible registered instructions could include:
   a. "*Private Sector dissemination limited to persons responsible for the security of the [blank] facility*";
   b. "*dissemination only to law enforcement personnel*";
   c. "*dissemination only to persons assigned to the [blank] case*"; or
   d. "*dissemination only to persons with a background check in accordance with [blank]*" (In examples a, c, and d, a single dissemination instruction, registered in the CUI Registry, would cover multiple documents, each of which might have the blank filled in differently).
3. Shall be in compliance with department and agency policies that specify, by position, which officials are authorized to restrict dissemination only to named individuals. These policies will be registered with the CUI Executive Agent by the department or agency head.
4. May provide contact information for the person or office that would approve access beyond the scope of the dissemination instruction. In cases where dissemination is limited to named individuals, such contact information is mandatory. (For example, instructions limiting dissemination of proprietary data to individuals who have signed a non-disclosure agreement (NDA) would identify the contact person or office for requesting additional NDAs.)

The CUI Executive Agent will define and establish standards for Specified Dissemination instructions.

IV. CUI Governance Structure

The success of the new CUI Framework depends upon an empowered governance structure with clearly defined and well understood business processes. The governance structure will be composed of a central management and oversight authority and participating Federal departments and agencies. Within the limits of the law, State, local, tribal, and private sector representatives shall also participate in an advisory capacity. The CUI Executive Agent may provide advisory guidelines to assist State, local, tribal, and private sector entities with implementation of the CUI Framework.

The President has designated NARA as the CUI Executive Agent. In this role, NARA will develop and issue standards for the CUI Framework and will conduct a periodic review of the CUI Framework and adjust, as required, based on input from heads of Federal departments and agencies, the CUI Council and the Legislative Branch. And NARA will serve as a spokesperson to Congress, the media, special

interest groups, professional organizations, and the public for matters related to the management and governance of CUI.

In addition, NARA will establish and maintain the CUI Registry for CUI markings, and safeguarding and dissemination instructions. In coordination with the heads of departments and agencies, NARA will establish the standards for and approve "Specified Dissemination" instructions, as defined by the heads of departments and agencies, and list them in the CUI Registry. The CUI Registry will be publicly available unless information in the registry (e.g., specific instructions relating to the permitted dissemination of information) is itself designated and marked as 'CUI'.

NARA will receive advisory support from a CUI Council, which shall act as a subcommittee of the ISC, created by IRTPA. The CUI Council members shall be drawn from the ISC's membership.[5] Representing the needs and equities of ISE participants, the CUI Council will provide advice and recommendations to the CUI Executive Agent on ISE-wide CUI policies, procedures, guidelines, and standards. As appropriate, the CUI Council will consult with the ISC's State, Local, Tribal, and Private Sector Subcommittee. NARA will work with the CUI Council to identify properly qualified personnel from participating departments and agencies who will contribute, for a limited amount of time, to the operational capabilities of the CUI Executive Agent. The department and agency detail to the host agency will last for a period of time necessary for the stand-up of the Executive Agent, as determined by the CUI Council and Executive Agent.

Heads of all Federal departments and agencies will be responsible for implementing the CUI Framework standards for ISE-wide CUI policy and ensuring that their departments or agencies comply with the CUI Framework.

Detailed descriptions of the roles and responsibilities of the CUI Governance Structure are found in the President's Memorandum on the Designation and Sharing of Controlled Unclassified Information.

V. CUI Exceptions

The Presidential Memorandum requires that all CUI originated by Federal departments and agencies and shared within the ISE shall conform to the policies and standards for the designating, marking, safeguarding, and disseminating established herein. However, certain important infrastructure protection agreements between the Federal government and the private sector are not fully accommodated under the current CUI Framework. As a result, the following existing Federal Regulations with their associated markings, safeguarding requirements, and dissemination limitations will be excluded from the CUI Framework:

- 6 CFR Pt. 29 – PCII (*Protected Critical Infrastructure Information*)
- 49 CFR Pts. 15 (*DOT*) & 1520 (*DHS/Transportation Security Administration) – SSI (Sensitive Security Information*)
- 6 CFR Pt. 27 – CVI (*Chemical Vulnerability Information*)
- 10 CFR Pt. 73 – SGI (*Safeguards Information*)

CUI Marking

The affected department or agency will have the flexibility to choose the most applicable CUI safeguarding marking ("Controlled" or "Controlled Enhanced") for the regulation. Any additional requirements for the safeguarding beyond that specified under the CUI Framework will be registered in the CUI Registry, maintained by the CUI Executive Agent. When marking a document, the regulatory marking will follow the CUI marking and a Specified Dissemination instruction will articulate any additional regulatory requirements.

For example:

---

[5]As necessary, the CUI Executive Agent may from time to time invite additional departments or agencies to participate on the CUI Council

Controlled Enhanced\Safeguards Information (Listed in the CUI Registry: SGI must be processed on a stand-alone computer or computer system with appropriate Federal Information Processing Standards encryption.)

Specified Dissemination: Dissemination only to authorized nuclear sector personnel. (Listed in the CUI Registry: "Authorized nuclear sector personnel" is defined as follows...)

CUI Safeguarding and Dissemination

All specific safeguarding and dissemination requirements for the excepted markings will be listed in the CUI Registry. An individual who receives PCII, SSI, CVI, or SGI will be expected to refer to the CUI Registry for details on handling this information.

CUI Governance Structure

The excepted markings (and their associated safeguarding requirements and dissemination limitations) will be subject to the CUI governance processes. Departments and agencies with these excepted markings will participate in the CUI Council. Any proposed revisions to the PCII, SSI, CVI, and SGI will be done in coordination with the CUI Governance Structure.