Controlled Unclassified Information:

Recommendations for Information Control Reform



Acknowledgements

This OMB Watch report was written by Sean Moulton, Roger Strother, and Chris George. We thank the following individuals for their feedback on the report during drafting: Meredith Fuchs, National Security Archive; Steven Aftergood, Federation of American Scientists; Sharon Bradford Franklin, Constitution Project; Michael German, American Civil Liberties Union; Patrice McDermott, OpenTheGovernment.Org; and Danielle Brian, Project on Government Oversight. While these individuals provided input and edits on our recommendations, their assistance does not necessarily constitute support of the final product.

Executive Summary

While many people probably have a general grasp of the meaning and importance of classified information, most probably don't know the meaning of Controlled Unclassified Information (CUI), Sensitive But Unclassified information (SBU), or the host of other non-classified labels. Unfortunately, too many of the people who are confused about these information categories work for the very agencies using the labels.

The CUI and SBU (an earlier catch-all term that often referred to any and all labels that were not part of the official classification system) are typically categories of records that need special handling to protect the information from inadvertent disclosure. For example, the records may contain privacy information or details about an ongoing investigation.

The labels were meant to make government employees' jobs easier. However, as the number of different labels grew over the years, fewer and fewer people understood exactly what restrictions applied to each label.

The lack of confidence and certainty about how information stamped with such labels should be handled results in officials shutting down almost all access to the data by anyone else. Thus, in attempting to prevent possible misuse of the information, the government has often prevented any timely legitimate use of the records, as well. Other federal agencies, state officials, local law enforcement, and the public get locked out and never fully benefit from information the government has spent taxpayer dollars collecting.

Failures of government agencies to connect the dots between different pieces of information held by different agencies highlighted the fact that "over-protection" of records could easily lead to under-use of the information.

In May 2008, President George W. Bush issued a memo that replaced the numerous SBU labels with a uniform designation entitled "controlled unclassified information" that contained three tiers of safeguarding procedures and dissemination controls. The goal was to standardize practices and thereby improve the sharing of information among government officials. However, there are several other well known SBU problems that were left unaddressed by Bush's memo, such as the need to reduce the amount of information with such control markings and the need to improve public disclosure of information that does not need to be withheld. If the problems remain unaddressed, we will miss a major opportunity to overhaul a problematic system.

Just a few months after taking office, President Barack Obama issued a memo on classification and SBU that reopened the door on the process of overhauling these unclassified information categories. Obama created an Interagency Task Force to review SBU practices, create metrics for measuring agency progress implementing the CUI framework, and within 90 days, report back with recommendations on how to proceed.

This report attempts to outline the problems associated with SBU information categories and the current process to reform them into a simpler, more manageable system. We offer clear recommendations to the Task Force and the Obama administration on how to address these issues.

The most expedient method to address the CUI problems would be a memo from Obama that would amend the original instructions and clarify any issues that went unaddressed in the Bush memo. We urge the interagency task force to recommend the creation of a new CUI policy with these problems in mind.

If properly implemented, the CUI framework should improve management of information, reduce the number of different control labels used, and reduce the amount of information being categorized so the system can operate more effectively. The new memorandum should also seek to maximize disclosure to the public by prohibiting reliance on control labels in making FOIA determinations, requiring portion marking of records to allow greater use of partial disclosures, and establishing time limits on labels that would allow the records to be more widely shared after the period of sensitivity has passed. Oversight of the program, such as audits and regular reports by agencies, should be embraced to ensure the reform efforts don't mistakenly cause even greater overuse of control labels.

The CUI framework should also include requirements for training and enforcement to drive timely implementation. Additionally, clear policies are needed to protect whistleblowers who disclose CUI records to uncover waste, fraud, and mismanagement.

Sean Moulton, Director, Federal Information Policy OMB Watch

The Origins of Sensitive But Unclassified Information

The Cold War led to a considerable restructuring of the United States government. The modern national security and intelligence apparatus was created to address the challenges and threats of a bipolar world in which the United States and the Soviet Union were dominant superpowers. A variety of disparate intelligence services were created with specific missions. Each fiercely protected its individual turf, and there was little occasion or impetus for information sharing between agencies. Furthermore, there was little reason for cooperation between agencies with a foreign or domestic focus when national security threats were perceived as external.

In this environment, there were a variety of policies implemented to protect information, both at the level of the individual agencies and across the federal government. Classification was created and expanded by Executive Order to protect nuclear secrets and other information pertinent to national security. In the 1970s, agencies began to identify sensitive but unclassified information (SBU) that did not meet the criteria for classification but nonetheless was thought to need more secure handling to prevent inadvertent disclosure. A multitude of SBU designations proliferated, eventually reaching more than 100 markings across the federal government, including such labels

as For Official Use Only (FOUO), Security Sensitive Information (SSI),¹ and Law Enforcement Sensitive (LES).

Four principal SBU problems complicated information sharing across the government. First, SBU categories were vaguely defined and unevenly implemented across government agencies. Second, authority to mark documents as sensitive was so decentralized within agencies that often virtually anyone employed by the agencies could label information, including government contractors. Third, government agencies have sometimes incorrectly interpreted SBU as being automatically exempt from requests under the Freedom of Information Act (FOIA) and other information disclosure and sharing processes. Fourth, the SBU categories had no time limits on how long information was to remain controlled and no review procedures to improve implementation over time.² These problems resulted in a confusing system that excessively applied the SBU category and permanently restricted all information.

SBU has become a more significant concern in recent years. A March 2002 memorandum by White House Chief of Staff Andrew Card instructed departments and agencies to control not only classified information, but "other information that could be misused to harm the security of our nation and the safety of our people." This was consistent with the Bush administration's tendency to maximize information withholding and led to an increased use of SBU labels.

The Homeland Security Act of 2002 authorized the Department of Homeland Security (DHS) to label and protect sensitive information – though it remained undefined – and share it with local and state government entities and relevant individuals in the private sector, provided that they sign nondisclosure agreements. This legislation provided an extraordinary amount of discretion to DHS and further contributed to a culture of "when in doubt, withhold." DHS issued a May 2004 directive requiring employees to mark as "For Official Use Only" any "sensitive but unclassified information" generated or received by DHS.⁴

Thus, the multitude of SBU categories, agency subjective definitions, and unclear disclosure policies created a breeding ground for unchecked government secrecy. Over several years and numerous investigations, the Government Accountability Office found that agencies lacked clear policies, oversight, and training on handling sensitive information. This lack of uniform meanings for information labels and dissemination standards across agencies created great uncertainty in if and how information could be shared and with whom, which resulted in increased withholding.

-

¹ SSI is one category of SBU that was not created at the discretion of an agency, but by statute. It has its origins with the Air Transportation Security Act of 1974, which permitted the FAA to not disclose information that would violate privacy, reveal trade secrets, or reduce safety.

²Information classified in accordance with Executive Order 12958, as amended, is much more vigorously regulated. Only a select group with proper training and security clearances are permitted to classify documents that fall within a strict definition of eligibility. There is additionally an automatic declassification date depending on the level of classification, set at no more than 10 years from the original classification. Only after review can this original period be extended, and only for information fitting established criteria.

³ Andrew H. Card, Jr., "Action to Safeguard Information Regarding Weapons of Mass Destruction and Other Sensitive Documents Related to Homeland Security," Memorandum for Heads of Executive Departments and Agencies, http://www.usdoj.gov/oip/foiapost/2002foiapost10.htm

^{4 &}quot;SBU – Sensitive But Unclassified Information, and FOUO – For Official Use Only," Coalition of Journalists for Open Government, http://www.cjog.net/background_sbu_sensitive_but_unclass.html

Critiques of Information Sharing

In October 2007, the National Strategy for Information Sharing identified several core principles:

- Effective information sharing comes through strong partnerships among Federal, State, local, and tribal authorities, private sector organizations, and our foreign partners and allies;
- Information acquired for one purpose, or under one set of authorities, might provide unique insights when combined...with seemingly unrelated information from other sources, and therefore we must foster a culture of awareness in which people at all levels of government remain cognizant of the functions and needs of others and use knowledge and information from all sources to support counterterrorism efforts...⁵

However, the goal of increased and improved information sharing in the United States government is hardly new. A need for reform along the lines of similar ideals has been echoed for the last three decades. In 1975, as activities of the intelligence community during the Vietnam War and the Nixon administration were being investigated, the White House prepared a briefing book on potential reforms and recommended actions for President Gerald Ford. In the first paragraph, it is noted, "Critics outside the Administration and Community leaders have recognized the need to improve protection of secrecy and, at the same time, to provide for wider dissemination of intelligence product to those who have a need to know." This is the essential conundrum of information sharing: how to provide for greater exchange of information while still securing sensitive information from those who would use it for detrimental purposes.

Despite this early identification of a problem, information sharing did not receive serious attention until after the terrorist attacks of Sept. 11, 2001. The National Commission on Terrorist Attacks Upon the United States – "the 9/11 Commission" – identified a critical failing in the months before the attacks: "Information was not shared, sometimes inadvertently or because of legal misunderstandings. Analysis was not pooled.... Often the handoffs of information were lost across the divide separating the foreign and domestic agencies of the government." Structural barriers, a lack of common standards, and excessive complexity and secrecy were cited as impediments to a unified effort in intelligence gathering and analysis. They proposed not only a reorganization of the intelligence community, but the creation of an information network linking government agencies and a seismic shift in the culture of information.

Cold War security practices were found to "nurture overclassification and excessive compartmentation of information among agencies.... Agencies uphold a 'need-to-know' culture of information protection rather than promoting a 'need-to-share' culture of integration." A standard of information sharing is needed not only between agencies of the federal government, but across levels of government. Prevention of and response to future emergencies requires coordination among federal agencies with both foreign and domestic focus and law enforcement officials, health care workers, and other emergency response services in the communities themselves. This level of

⁵ National Strategy for Information Sharing: Successes and Challenges In Improving Terrorism-Related Information Sharing, October 2007, 2-3.

⁶ Dick Cheney, Intelligence Community Decision Book for the President, http://www.fas.org/irp/eprint/ford-intel.pdf

⁷ Final Report of the National Commission on Terrorist Attacks Upon the United States, <www.9-11commission.gov>, 353

⁸ Final Report of the National Commission on Terrorist Attacks Upon the United States, 417.

coordination was not possible when each agency independently set standards for controlling information it possessed.

SBU was part of the information sharing problem. Organizational cultures favored greater control over information rather than greater disclosure. Through decentralized control of marking procedures, the number of designations and their use proliferated. Without consistent handling practices between agencies, confusion reigned over who would have the authority to view what information. And in the end, necessary information was not being sent to the relevant agencies.

<u>Implementation of Controlled Unclassified Information</u>

To improve the sharing of homeland security information, the Intelligence Reform and Terrorism Prevention Act of 2004 required the president to establish an Information Sharing Environment with uniform policies and standards across levels of government, including key components of the private sector. Bush issued a December 2005 memorandum directing that SBU be standardized across the government and established an interagency Sensitive But Unclassified Coordinating Committee. Bush eventually issued a May 2008 memo, replacing the multiple SBU categories with a uniform designation entitled "controlled unclassified information."

The memo defined controlled unclassified information (CUI) as:

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.⁹

Within the CUI designation, the memo established a three-tiered system of safeguarding procedures and dissemination controls: Controlled with Standard Dissemination, Controlled with Specified Dissemination, and Controlled Enhanced with Specified Dissemination. Agencies were prohibited from creating any additional labels. This memo ostensibly intended "to standardize practices and thereby improve the sharing of information, not to classify or declassify new or additional information." However, as the Information Sharing Environment is specific to terrorism-related information, a vast quantity of SBU information was left unaddressed.

The Bush memo assigned responsibility for the implementation of CUI to the National Archives and Records Administration (NARA). As "Executive Agent," NARA is responsible for developing standards and implementation guidance, monitoring compliance, establishing training, and creating enforcement mechanisms and penalties. A new CUI office was created under the Information Security Oversight Office, which was created in 1978 to oversee the classification system. While NARA is principally concerned with the preservation of historical documents rather than management of current records, the agency's dedication to information preservation and objectivity was seen as critical to the new program's objectives.

On May 27, 2009, Obama issued his own memorandum calling for a review of classification policy and controlled unclassified information. This new memo states "the process of implementing the

⁹ President George W. Bush, "Designation and Sharing of Controlled Unclassified Information (CUI)," Memorandum for the Heads of Executive Departments and Agencies, May 9, 2008.

new CUI Framework is still ongoing and is not expected to be completed until 2013."¹⁰ The memo encourages relevant agencies to continue the implementation of CUI but recognizes that "new measures should be considered to further and expedite agencies' treatment of SBU information and information sharing."¹¹ Pursuant to this goal, the memo creates an Interagency Task Force to review SBU practices, create metrics for measuring agency progress implementing the Framework, and within 90 days, report back with recommendations on how to proceed *vis-à-vis* CUI.

Concerns with Implementation

The current CUI effort makes progress in simplifying the framework and establishing consistent definitions and practices but falls far short in other areas. Serious questions remain regarding the overuse of CUI markings, time limits and implications for public access to the information, state fusion centers, checks and balances in the federal government, and the narrow focus of the Bush memorandum. These concerns remain unaddressed in Obama's memorandum, and we urge the Interagency Task Force to consider them in making its report to the president.

Amount of Information & Overuse

The existing CUI Framework established by the Bush memorandum makes no effort to limit the use of control designations. The definition of CUI remains vague and overly broad, with no public interest balancing test that might prevent critical information from disappearing into this category. There is also no provision limiting the number of officials capable of assigning these markings. In the past SBU labels have been overused by officials, contractors, and even regulated entities who were able to apply such labels to information they were submitting to government agencies. There is also only cursory mention that CUI designations should not be used to conceal information on waste, fraud, or abuse, nor should they be assigned to information that is already public.

The government already knows that use of numerous SBU designations was continuously increasing, which directly contributed to information sharing problems. While the framework of control labels as designated by the memorandum is a step forward, it does not prioritize reducing their use. True information sharing is best accomplished by eliminating unnecessary controls.

Moreover, the CUI designations in the Bush memorandum are only required for terrorism-related information. It is difficult, if not impossible, to segregate "terrorism-related information" from other kinds of information, and it is highly questionable if the effort to separate the information is useful. For instance, the Department of Energy (DOE) uses the control label "Unclassified Controlled Nuclear Information." Since it is feasible that such information would be useful to terrorists, it is impossible to know for certain if information labeled as UCNI qualifies as "terrorism-related."

There is a great deal of sensitive, non-terrorism-related information that, if shared more readily between agencies and officials throughout government, would benefit the public interest. When information is shared, agencies are better able to connect the dots and address previously unnoticed issues and unanticipated threats. Restricting the information-sharing improvements to terrorism-related information, leaves other sensitive information still mired in the same problems, unable to be fully shared or used. A new CUI regime that solves such information sharing problems

-

¹⁰ President Barack Obama, "Classified Information and Controlled Unclassified Information," Memorandum for the Heads of Executive Departments and Agencies, May 27, 2009, 3.

¹¹ Ibid.

and addresses other problems such as over use and should not be limited to terrorism-related information, but should be applied to the whole of the executive branch. However, as the efforts to tackle the information sharing problems could be overwhelmed by trying to immediately address all types of sensitive information, the current limitation of the CUI policy to terrorism-related information may be a practical approach to testing new policies before expanding them.

Public Access & Time Limits

Certain CUI provisions could interfere with public access to material that should be released. The Framework does not mandate a length of time after which such CUI designations on a document would expire. This is particularly strange since classified information is automatically declassified after a predetermined period unless officials intervene. Further, the Bush memorandum states that CUI labels "may inform but do not control" the decision to disclose designated material under FOIA. However, it can be assumed that agency employees will likely favor withholding the material. Information labeled CUI, just as SBU before it, could remain controlled indefinitely, keeping records out of the public domain, even if there is no justifiable reason to do so. This has raised concerns that CUI is merely a fourth classification level, albeit one with no recourse for public access in the present or future. Further, the lack of time limits on material designated as SBU or CUI presents a major problem for the long-term archiving of records. CUI is not a vehicle for withholding information, but it is a system established to enable information sharing and to prevent the restriction of information that should not have been controlled to begin with.

Checks & Balances

The Bush memorandum policies do not clarify that congressional and court oversight qualify as "official government use," nor do they indicate that Congress and the courts should freely receive CUI records. In the past, agencies have used control labels to deny information to legislative offices and courts. When agencies have release SBU information to Congress, they have often placed restrictions on use and sharing. If uncorrected, agencies could use control labels to limit the use of records in public hearings and inquiries, thereby undermining the constitutional role of Congress to serve as a principal check and balance in the federal government and to conduct oversight of the executive branch.

Additionally, the judicial branch often defers to executive agencies in decisions concerning secrecy claims. This is especially true on matters related to the president's powers as commander-in-chief. Unless policies establish procedures for courts to review and challenge CUI information, the third branch of government will not be able to be the unbiased arbiter checking executive branch excesses.

Enforcement

SBU and CUI inhibit collaborative government processes. Data classification schemes that cannot be applied government-wide prevent agencies from sharing valuable information that could otherwise help government to work more effectively and efficiently. Very little, if any, oversight exists to control the pandemic spread of control labels. NARA has very little enforcement capacity and is often unwilling to utilize what authority it does have.

Often, proper training would preclude the need to use enforcement mechanisms. Due to lack of training and inadequate guidance, officials and employees making disclosure decisions or classification determinations are not fully aware of all related policies and requirements. In some

situations, poorly informed decisions can be corrected through appeals, but these cost time and money to pursue.

* * *

Controlled unclassified information has the potential to be a significant improvement on sensitive but unclassified information labels. It provides a consistent framework for the handling of terrorism-related information across the government. But as presently constituted, it fails to avoid many of the pitfalls that have historically plagued SBU. Serious concerns remain regarding the overuse of CUI labels, time limits and public access, state fusion centers, separation of powers, and the narrow focus of CUI. Significant efforts are needed by the CUI Office at NARA and by the Congress to insure that CUI achieves its goals of enhancing information sharing and does not result in the restriction of additional information. The May 27 Obama directive on overclassification and the CUI/SBU problem marks the hopeful beginning of a process to enable real change. However, the memo does not recognize all the problems detailed in this report. The task force should review these problems and seek to rectify them with the recommendations it delivers to the president.

Recommendations for Implementation

Most of the problems currently associated with the CUI efforts derive from deficiencies in President Bush's CUI memo that laid out the scope and approach to the program. It may be possible for NARA to correct some, or even all, of the shortcomings through careful development of guidance for agencies and oversight of implementation. However, such an approach would likely be mired with disagreement over NARA's authority to make decisions that are not explicitly described in the original memo. The most expedient method to address the current concerns with CUI would be a memo from Obama that would clarify these authority issues and amend the original instructions. New agency policies that govern CUI/SBU and which are publicly available need to be established. We hope that the interagency task force established by Obama's May 27 directive will recommend that he create a new CUI policy with these problems in mind.

Amount of Information & Overuse

If properly implemented, the CUI framework should improve management of information, reduce the number of different control labels used, and reduce the amount of information being categorized so the system can operate more effectively. Unfortunately, the current effort perpetuates unchecked secrecy. It does not prioritize reducing the use of control labels, and it runs the risk of undermining FOIA and appropriate disclosure of information to Congress. True information sharing is best accomplished by eliminating unnecessary information controls, and experience shows that when there are no incentives to reduce secrecy, too much information is kept hidden. Moreover, the limitation of "terrorism-related" information is too narrow and potentially prevents other information not immediately recognizable as relevant from being shared efficiently. Thus, the memorandum should enforce the three-tiered designation system on all CUI information. This system would have other added benefits in increasing information sharing across agencies. Federal, state, and local governments will be in a better position to react promptly to other risks, such as the recent H1N1 influenza scare.

• The purposes of control markings should be clarified: (1) to facilitate information sharing so information can pass from an agency to another agency, state, local, or tribal authorities, as well as the public; and (2) in limited

circumstances, to protect extremely sensitive information that agencies have been directed to safeguard by a statute or a presidential policy.

- The memo should make it a goal of the new program to eventually expand the CUI effort to cover all non-classified information that agencies believe require labels. Implementation for terrorism-related information should be closely monitored and once officials are sure the new policies are not being overapplied and that they maximize information sharing and public access, efforts should be made to expand the policy, or some version of it, to all sensitive unclassified information.
- The memo should affirm that a goal of the program is to reduce the amount of
 information that is labeled CUI and provision that will help limit such
 restrictions should be included such as limiting the number of individuals who
 have authority to mark records as CUI.
- The new memo should establish that one measure of the CUI program will be how much new information is made available to the public.
- In the new memo, the president should establish more defined criteria of information that can be designated as CUI. This should include a timeline for the eventual inclusion of all sensitive but unclassified information into the CUI system.
- The memorandum should also prohibit the designation of information that is already public as CUI.

Public Access & Time Limits

Though CUI does not change the requirements of FOIA, it is likely that, without clear procedures and criteria to properly evaluate CUI records, agency employees will often withhold such records. CUI is a handling instruction and should hold no consequence on decisions of public disclosure under FOIA since, even with reforms, there is a greater chance of CUI designations being applied to an overly broad number of records. Further, CUI designations, unlike classification designations, do not have set expiration dates, leaving disclosure at the absolute discretion of agency personnel.

- The new memo should prohibit reliance on control labels in making FOIA determinations, emphasizing that the CUI Framework and FOIA are entirely separate and that CUI labels have no bearing on whether records are exempt from disclosure under FOIA.
- To maximize disclosure, the memo should require agencies to, wherever possible, use portion marking of records so partial disclosures can be more readily implemented.
- The memo should also establish a time limit of no more than five years, after which CUI markings will automatically expire unless renewed by the agency that produced the record. We understand that time limits may have to fluctuate based on the type of information being controlled; thus, agencies should have to

justify why a specific document is controlled for a given length of time. When renewing markings, agencies should have to justify why the information still requires control.

Checks & Balances

The president should ensure that control labels do not interfere with the checks and balances provided by the judicial and legislative branches. In fact, new and complicated programs, such as the CUI effort to reform all non-classified information labels, need even closer oversight to ensure no disruptive unintended consequences develop. The president should embrace this oversight and establish provisions that enable it to occur easily and without agency obstruction.

- The new memo should specify that judicial deference not be given to control labels, and documents should be reviewed based solely on content.
- The memo should also recognize that congressional activity constitutes "official
 use" and that no control labels should justify withholding information from
 Congress. The memo should also state that CUI is not to interfere with
 congressional affairs by restricting the legislative branch's ability to disclose or
 redistribute material.
- For CUI categories created statutorily that include restrictions on government use, such as Critical Infrastructure Information, the president should seek revisions from Congress to allow maximum flexibility in the government's ability to use and share such information.

Enforcement

The President should create a CUI framework with requisite enforcement mechanisms but should work with Congress to implement these changes long-term. These mechanisms should include penalties for employees and contractors who repeatedly fail to comply with CUI policies and for employees and contractors with original classification authority who repeatedly fail to comply with proper classification policies. The government also needs to do a better job of getting the decision right the first time through better training. Successful completion of training and education programs will be counted as a positive factor for employment, evaluation, and promotion decisions.

Procedures to monitor the use of CUI and to ensure compliance will be vital to preventing the use of CUI to mask waste, fraud, and abuse. Appropriate consequences for employees and contractors who misuse the label are also a necessary component. Such penalties would be the flip-side of the criminal prohibition against unauthorized disclosure and should be imposed only after an employee or contractor has been notified of non-compliance and has gone through retraining. As a corollary, there should be adequate protections put in place for whistleblowers who bring such activities to light. None of the previous recommendations are necessarily difficult to institute, but none will succeed without proper enforcement.

• The president's new CUI memo should grant NARA clear enforcement authority to restrict the amount of CUI by removing markings and releasing information. To bolster the enforcement authority of NARA, the president should consider adding OMB to the enforcement and oversight process.

- The memo should make clear that whistleblowers disclosing CUI records to uncover waste, fraud, and abuse will be protected from reprisal.
- To preclude the need to activate enforcement mechanisms, the president should establish mandatory training for agency officials on transparency requirements and policies to ensure better implementation, including specific training for employees and contractors with classification authority and responsibility for implementing the framework on CUI. There should be some mechanism for monitoring this system to ensure compliance.

* * *

Controlled unclassified information has the potential to be a tremendous improvement over the disparate collection of sensitive but unclassified information labels that complicate information sharing. However, this will only be the case if steps are taken to address the identified problems with CUI and if appropriate solutions are instituted. We hope that the task force takes these recommendations into account when submitting its final recommendations to the president. Any new directives, regulations, or guidance promulgated to implement the CUI framework should be made available to the public to increase understanding of what control labels indicate and to increase the likelihood that such measures are narrowly tailored.