July 7, 2015

Kimberly Keravouri
Information Security Oversight Office
National Archives and Records Administration
Suite 4100, 8601 Adelphi Road
College Park, MD 20740-6001

Re: Comments on Proposed CUI Federal Regulation (CFR 2002)

Dear Ms. Keravouri:

The undersigned organizations write to provide comments on the proposed Federal Regulation by the Information Security Oversight Office (ISOO) on Controlled Unclassified Information (CUI). We have coordinated closely with ISOO as it has worked to implement the CUI framework, and we greatly appreciate the office's responsiveness to our concerns and suggestions along the way. We nonetheless have some remaining concerns that certain provisions of the proposed rule could discourage legitimate information-sharing, both internally and outside the government. Accordingly, we submit the following comments that are designed to ensure CUI does not become a fourth level of classification, contrary to the spirit and intent of Executive Order 13556, or hinder public access to government records pursuant to the Freedom of Information Act.

A. Comments

Subpart A – General Information

§ 2002.1 Purpose and scope.

We suggest removing the word "sensitive," which implies a fourth level of classification rather than information that is subject to a range of controls for a variety of reasons. Copyrighted information, for example, is not necessarily "sensitive," but is considered CUI. Therefore, we suggest the following changes to subsection (b):

(b) The CUI Program standardizes the way the executive branch handles ~~sensitive~~ *certain* information that requires ~~protection~~ *special controls* under laws, regulations, or Government-wide policies, but that does not qualify as classified under Executive Order 13526, Classified National Security Information, December 29, 2009 (3 CFR, 2010 Comp., p. 298), or the Atomic Energy Act of 1954 (42 U.S.C. 2011, *et seq*), as amended.

Similarly, in subsection (e)(2), we suggest the language relating to sensitive information be removed, and the paragraph instead read as follows:

(2) Other non-executive branch entities. When feasible, executive branch agencies should enter formal information-sharing agreements and include a requirement that any non-executive

branch party to the agreement comply with the Order, this part, and the CUI Registry. When an agency's mission requires it to disseminate CUI without entering into an information-sharing agreement, the agency must communicate to the recipient that ~~because of the sensitive nature of the information,~~ the Government strongly encourages the non-executive branch entity to protect CUI consistent with the Order, this part, the CUI Registry, *and other applicable statutes or regulations.*

We also have concerns that the restrictions on disclosure set forth in this rule could be interpreted to override policies that implement discovery obligations in litigation, whistleblower protections, and other lawful disclosures. Our understanding from conversations with ISOO is that the rule is not intended to affect existing rights or responsibilities with respect to such disclosures. The proposed regulation is silent on the Whistleblower Protection Act of 1989 and related statutes, which could create confusion and a corresponding chilling effect, as well as unnecessary personnel disputes and associated litigation.

There is no lawful basis for anything besides a clear boundary. Section 2(b) of EO 13556 provides,

(b) The mere fact that information is designated as CUI shall not have a bearing on determinations pursuant to any law requiring the disclosure of information or permitting disclosure as a matter of discretion, including disclosures to the legislative or judicial branches.

The whistleblower laws all are discretionary disclosure statutes. Further, this year in a 7-2 decision, *MacLean v. Department of Homeland Security,* 135 S. Ct. 913 (2015), the Supreme Court overturned the dismissal of an employee for publicly releasing CUI, in that instance Sensitive Security Information, because the termination violated the Whistleblower Protection Act.

We therefore suggest adding a new subsection (i) that would read:

(i) Nothing in this part is intended to limit lawful and/or protected disclosures to law enforcement officials, Inspectors General, or the legislative or judicial branches or elements thereof, or to preempt, override, or otherwise affect legal protections for disclosures by whistleblowers as set forth in statute, regulation, or executive order or directive.

This language could alternatively be inserted as a new subsection (d) – entitled "Rule of Construction" – to Section 2002.13 (Access and Disseminating). Finally, it could be the contents of a new provision, **§ 2002.28, CUI, the Whistleblower Protection Act and related statutes.** However organized, the regulation must be clear that CUI status does not affect the rights and responsibilities of these laws.

§ 2002.2 Definitions.

On "misuse of CUI," additional language in this definition would help make clear that the use of CUI markings for information that does not qualify as CUI is inappropriate. In other words, it is not just the failure to apply proper controls to CUI that should be considered problematic, but the improper invocation of CUI and the unwarranted restrictions on information-sharing that may result. In order to make this clear, we suggest the definition read:

Misuse of CUI occurs when someone uses CUI *or applies CUI markings* in a manner inconsistent with the policy contained in the Order, this part, and the CUI Registry, or any of the laws, regulations, and Government-wide policy that establish CUI categories and subcategories. This may include intentional violations or unintentional errors in *marking*, safeguarding or disseminating CUI.

On "unauthorized disclosure," we note that "lawful Government purpose" should apply to the distributor of information, not the recipient. A private citizen or organization, for example, may not have a lawful "Government" purpose, but that should not preclude the citizen or organization from receiving information if an agency has a lawful Government purpose for sharing it (as the proposed rule elsewhere contemplates when it states that CUI may be disseminated to non-executive branch entities, defined to include private organizations). We suggest the following changes:

Unauthorized disclosure occurs when individuals or entities *disseminate or permit access to CUI in a manner inconsistent with the restrictions set forth in this rule*. ~~that do not have a lawful Government purpose to access the CUI gain access to it~~. Unauthorized disclosure may be intentional or unintentional.

To clarify that private individuals as well as organizations should be eligible to receive CUI where appropriate, we also recommend that the definition of "non-executive branch entity" be amended as follows:

Non-executive branch entity is a person or organization established, operated, and controlled by individual(s) acting outside the scope of any official capacity as officers, employees, or agents of the executive branch of the Federal Government. Such entities may include elements of the legislative or judicial branches of the Federal government; State, interstate, Tribal, local, or foreign government elements; and private or international *persons or* organizations, including contractors and vendors.

§ 2002.4 Roles and responsibilities.

It is unclear from the current proposed rule who bears the responsibility of ensuring that CUI categories and subcategories remain up to date, reflecting only current laws, regulations, or Government-wide policies. To address this issue, we suggest adding a new subsection (a)(8) as follows (and renumbering the existing subsection (a)(8) and subsequent subsections accordingly):

(8) Reviews changes to law, regulation, or Government-wide policy authorizing CUI categories or subcategories, revises CUI categories and subcategories to reflect changed authorizations, and updates the CUI Registry accordingly.

Subpart B – Key Elements of the CUI Program

§ 2002.12 Safeguarding.

We are concerned that some of the specific safeguarding obligations in this section could pose barriers to timely access by authorized holders and are unduly onerous for some categories of CUI. We believe it should be sufficient to place clear responsibility on authorized holders to guard against authorized disclosure and provide specific examples of how such a responsibility could be discharged, without mandating each of these measures in every instance. For instance, the proposed rule currently "encourage[s]" rather than mandates the use of in-transit tracking of CUI that is transported or delivered; we believe this is a sensible approach that could be expanded.

Accordingly, we suggest the following changes. We recommend changing subsection (a) (1) as follows:

(a) General safeguarding policy.

(1) Agencies must safeguard CUI at all times in a manner that minimizes the risk of unauthorized disclosure while allowing for *timely* access by authorized holders.

In Subsection (c), we suggest the following changes:

(c) Protecting CUI under the control of an authorized holder. *Authorized holders must take reasonable precautions to guard against unauthorized disclosures of CUI. Adhering to the following measures would constitute taking reasonable precautions:*

(1) Authorized holders ~~must~~ have access to controlled environments in which to protect CUI from unauthorized access or observation.

(2) When discussing CUI, you ~~must~~ reasonably ensure that unauthorized individuals cannot overhear the conversation.

(3) When outside a controlled environment, you ~~must~~ keep the CUI under your direct control or protect it with at least one physical barrier. You or the physical barrier must reasonably protect the CUI from unauthorized access or observation.

(4) Agencies ~~must~~ protect the confidentiality of CUI that is processed, stored, or transmitted on Federal information systems consistently with the security requirements and controls established in FIPS Publication 199, FIPS Publication 200, and NIST SP 800-53.

In subsection (e) Reproducing CUI, we suggest the following change:

(2) When reproducing CUI documents on equipment such as printers, copiers, scanners, or fax machines, you ~~must~~ *are encouraged to* ensure that the equipment does not retain data or ~~you must~~ *to* otherwise sanitize it in accordance with NIST SP 800-53.

Finally, we suggest the following change in (f) Destroying CUI:

(2) When destroying CUI, including in electronic form, you ~~must~~ *are encouraged to* do so in a manner that makes it unreadable, indecipherable, and irrecoverable, using any of the following:

§ 2002.13 Accessing and disseminating.

A person who has a lawful Government purpose for disseminating information cannot guarantee in every instance that this purpose will be "furthered" by dissemination, as this may depend on the recipient's actions or other factors outside the disseminator's control. In subsection (a) General policy, therefore, under part (1), we suggest the following change:

(ii) ~~Furthers~~ *Is consistent with* a lawful Government purpose;

We also are concerned that the proposed rule allows the use of limited dissemination controls any time such controls serve a lawful Government purpose. The heart of the CUI program is the notion that legitimate controls must stem from law, regulation, or Government-wide policy. While these instruments may not articulate the specific dissemination controls necessary to implement their restrictions, this problem is better addressed by allowing the use of such controls only where required *or permitted* by the underlying instrument. We therefore propose the following change to subsection (b)(3) Limited Dissemination:

(ii) Use of limited dissemination controls to unnecessarily restrict access to CUI is contrary to the stated goals of the CUI Program. You may therefore use these controls only ~~when it serves a lawful Government purpose, or~~ *if* you are required *or permitted* by laws, regulations, or Government-wide policies to do so.

§ 2002.14 Decontrolling.

The current proposed rule frames decontrol as optional in all instances, whereas in fact, decontrol should be required in certain cases – e.g., where there is no longer any basis for control in law, regulation, or Government-wide policy. Requiring decontrol of information in such situations will not create any obligation to sort through large volumes of archived material, as the obligation to re-mark decontrolled information is triggered only when that information is restated, re-used, or transferred to a private institution. We suggest the following changes to subsections (a) through (d):

(a) Agencies ~~may~~ *must* decontrol CUI that they have designated:

(1) When laws, regulations or Government-wide policies no longer require or *permit* its control as CUI;

~~(2) In response to a request by an authorized holder to decontrol it, if the agency is the designating agency;~~

(~~3~~2) When the designating agency decides to release it to the public by making an affirmative, proactive disclosure;

(~~4~~3) When the agency releases it in accordance with an applicable information access statute, such as the Freedom of Information Act (FOIA);

(~~5~~*4*) Consistent with any declassification action under Executive Order 13526 or any predecessor or successor order; or

(~~6~~5) When a pre-determined event or date occurs, as described in the decontrol indicators section of this part.

(b) Agencies also may decontrol CUI in response to a request to decontrol it, if the agency is the designating agency.

(~~b~~*c*) Decontrolling ~~may~~ *shall* occur automatically upon the occurrence of one of the conditions in paragraph (a) of this section. *Decontrol may also be accomplished* ~~or~~ through an affirmative decision by the designating agency.

[Renumber current (c) and (d) as (d) and (e), respectively]

We also recommend removing the current subsection (e), as information that no longer requires or permits control should be decontrolled automatically pursuant to the revised language suggested above.

In subsection (g), we recommend the following change to clarify that public release may be subject to future laws and policies as well as existing ones:

(g) Once decontrolled, any public release of information that was formerly CUI must be in accordance with ~~existing~~ *applicable law and* agency policies on the public release of information.

In subsection (k), we are concerned about prohibiting the decontrol of CUI for the purpose of "mitigating" unauthorized disclosures. Official disclosure is often an important and necessary response to the unauthorized disclosure of information and can even mitigate any resulting harm.

The Director of National Intelligence, for instance, determined it appropriate to declassify and release a substantial amount of classified information in order to help the public understand and contextualize Edward Snowden's unauthorized disclosures. We understand this provision of the proposed rule is intended to prohibit the decontrol of CUI as a means of hiding unauthorized disclosures and avoiding accountability for them. This goal would more clearly and narrowly be served by the following language:

(k) You must not decontrol CUI in an attempt to conceal, *or otherwise to* circumvent *accountability for*, ~~or mitigate~~ an identified unauthorized disclosure.

§ 2002.15 Marking.

We suspect that executive branch employees are more likely to misuse CUI markings for mundane bureaucratic reasons than to conceal wrongdoing. We therefore suggest the following change to subsection (a)(5):

(5) You must not mark information as CUI to conceal illegality, negligence, ineptitude, or other disreputable circumstances embarrassing to any person, any agency, the Federal Government, or any partners thereof, *or for any purpose other than adherence to the law, regulation, or Government-wide policy authorizing control*.

In subsection (a)(6), we note that there is a need for guidance as to the legal status of "legacy markings." Because the rule does not require such markings to be stricken, it creates some confusion as to whether (and, if so, for how long) they continue to have legal effect.

We also believe the CUI marking should include the date of designation. This is an easy addition that will help the agency to determine when decontrol is appropriate in cases where the person marking the information neglects to specify the decontrol date; where the relevant time frame for decontrol is changed after the information is marked; if a maximum time period for control is identified in the future; etc. We suggest adding a new subsection (e) as follows, and renumbering the current subsection (e) and subsequent subsections accordingly:

(e) <u>Date of designation (mandatory).</u> To facilitate decontrol, all media containing CUI must be marked with the date or dates on which the information was designated CUI.

Subpart C – CUI Program Management

§ 2002.21 Agency self-inspection program:

We believe a direct review of information designated CUI is critical to assessing whether agencies are properly implementing the CUI framework. We therefore suggest the following change to subsection (c)(1):

(1) Self-inspection methods, reviews, and assessments that serve to evaluate program effectiveness, measure the level of compliance, and monitor the progress of CUI implementation, *including a review of a representative sample of CUI generated by the agency*;

§ 2002.22 Challenges to designation of information as CUI.

We believe it is important that members of the public, as well as authorized holders of CUI, be able to challenge the information's status (as is the case with classified information). Moreover, in the context of classified information, formal challenges by authorized holders are exceedingly rare, suggesting that challenges of this nature must be affirmatively encouraged – not just allowed – and that an anonymous challenge option should be provided. Accordingly, we suggest the following changes to subsections (a) and (b):

(a) ~~Authorized holders of CUI~~ *Anyone* who, in good faith, believes that ~~its~~ *the* designation *of information* as CUI is improper or incorrect ~~should~~ may (*and authorized holders of CUI should*) notify the designating agency of this belief.

(b) Agency CUI senior agency officials must create a process within their agency to *encourage*, accept, and manage challenges to CUI status. At a minimum, this process must include a timely response to the challenger that:

. . .

(5) Ensures that challengers *who are authorized holders have the option of bringing such challenges anonymously, and that challengers who are authorized holders* are not subject to retribution for bringing such challenges.

We thank you for the opportunity to submit comments, and appreciate your consideration. For further information, please contact Patrice McDermott at OpenTheGovernment.org (pmcdermott@openthegovernment.org), Elizabeth Goitein at the Brennan Center for Justice (goiteine@mercury.law.nyu.edu), Tom Devine at the Government Accountability Project (TomD@whistleblower.org), or Scott Amey (scott@pogo.org), with any questions.

Sincerely yours,

Brennan Center for Justice
Federation of American Scientists
Government Accountability Project
National Coalition for History
National Security Counselors
OpenTheGovernment.org
Project On Government Oversight