August 4, 2011

Defense Acquisition Regulations System
Attn: Mr. Julian Thrash
OUSD(AT&L)DPAP(DARS)
Room 3B855
3060 Defense Pentagon
Washington, DC 20301-3060

Re: Department of Defense Proposed Rule, "Defense Federal Acquisition Regulation Supplement; Safeguarding Unclassified DoD Information (DFARS Case 2011-D039)"

The Constitution Project (TCP) submits this comment in response to the Department of Defense (DoD) notice of proposed rulemaking (NPRM) published in the Federal Register on June 29, 2011.[1] The stated purpose of the NPRM is to amend the Defense Federal Acquisition Regulation Supplement (DFARS) to add a new subpart and associated contract clauses addressing requirements for safeguarding unclassified DoD information.[2] TCP opposes the content and purpose of this proposed rule, and urges the DoD not to adopt it. On November 4, 2010, the President issued Executive Order 13556 which establishes an open and uniform program for managing unclassified information that requires safeguarding or dissemination controls.[3] The NPRM essentially constitutes an end run around the new controlled unclassified information registration process outlined in E.O. 13556, and contains objectionable provisions that treat unclassified information as if it were classified in direct contravention of the presumption of openness established by E.O. 13556. Such a proposed rule is inconsistent with the Executive Order and should be abandoned.

TCP is a nonprofit organization in Washington, DC that promotes and defends constitutional safeguards by bringing together liberals and conservatives who share a common concern about preserving civil liberties. The Constitution Project's bipartisan Liberty and Security Committee, launched in the aftermath of the September 11 attacks, includes members of the law enforcement community, legal academics, former government officials, and advocates from across the political spectrum who develop and advance proposals to protect civil liberties as well as our nation's security.

As part of this work, the Constitution Project's Liberty and Security Committee has released a report entitled *Reining in Excessive Secrecy: Recommendations for Reform of the Classification and Controlled Unclassified Information Systems*.[4] This report was written in

---

[1]Defense Federal Acquisition Regulation Supplement; Safeguarding Unclassified DoD Information, 76 Fed. Reg. 38,089 (June 29, 2011) [hereinafter NPRM] (to be codified at 48 C.F.R. pt. 204, 252).
[2]*Id.* at 38,089.
[3]Exec. Order No. 13,556, 75 Fed. Reg. 68,675 (Nov. 9, 2010) (E.O. 13,556 was first released on Nov. 4, 2010, and was published in the Federal Register five days later on Nov. 9).
[4]THE CONSTITUTION PROJECT, REINING IN EXCESSIVE SECRECY: RECOMMENDATIONS FOR REFORM OF THE CLASSIFICATION AND CONTROLLED UNCLASSIFIED INFORMATION SYSTEMS (2009) [hereinafter TCP CUI REPORT], *available at* http://www.constitutionproject.org/pdf/178.pdf.

response to President Barack Obama's May 27, 2009, memorandum[5] which directed the heads of several federal agencies to lead an Interagency Task Force on controlled unclassified information (CUI) and to make recommendations to reform the federal government's system for handling and sharing CUI.[6] In the *Reining in Excessive Secrecy* report, TCP urges the executive branch to reform the use of CUI to promote information sharing and to reinforce core constitutional principles including checks and balances and public accountability.[7]

TCP's report details how the lack of clarity and uniformity surrounding CUI designations has inhibited information sharing among agencies and among the branches of the federal government with serious consequences for national security and accountability.[8] CUI encompasses a category of documents that are sensitive but *unclassified*, and as such are subject to safeguarding protections that fall short of classified protections.[9] Over-use of CUI markings creates barriers to information sharing, undermines the effort to protect truly sensitive information, impedes the country's ability to safeguard its national interests, prevents government transparency and accountability, and creates confusion about the proper use and handling of CUI.[10] The report provides 18 recommendations for how to reform the CUI framework. These include recommendations that the President create a presumption of openness and information sharing in government, increase agency and congressional access to CUI materials, and establish a CUI framework with clear standards and procedures and mechanisms of accountability.[11]

In November 2010, President Obama responded to these concerns in E.O. 13556, which orders the creation of a new system for managing CUI to replace the earlier ad hoc, agency-specific system.[12] The new CUI framework emphasizes the openness and uniformity of Government-wide practice, and establishes a system in which new CUI categories and subcategories "shall serve as exclusive designations" for sensitive but unclassified documents.[13] Significantly, these categories must be established "pursuant to and consistent with applicable law, regulations, and Government-wide policies."[14]

DoD's NPRM seeks to address safeguarding requirements for unclassified DoD information. The NPRM is broad in scope; the DoD estimates that the rule will apply to approximately 76 percent of DoD's small business contractors.[15] DoD awarded contracts to

---

[5] 74 Fed. Reg. 26277 (June 1, 2009).
[6] TCP CUI REPORT, *supra* note 4, at 1.
[7] *Id.*
[8] *Id.* at 4.
[9] *Id.*at 4.
[10] *Id.* at 7-10. Federal agencies have developed over 100 types of CUI labels. *Id.* at 4. Many people believe that this contributed to America's unpreparedness for the September 11 attacks. *See* THE TASK FORCE ON CONTROLLED UNCLASSIFIED INFORMATION, REPORT AND RECOMMENDATIONS OF THE PRESIDENTIAL TASK FORCE ON CONTROLLED UNCLASSIFIED INFORMATION 7 (2009) [hereinafter CUI TASKFORCE REPORT].
[11] TCP CUI REPORT, *supra* note 4, at 13-16. *See also* CUI TASKFORCE REPORT, *supra* note 10 (echoing many of TCP's recommendations).
[12] Exec. Order No. 13,556, *supra* note 3.
[13] *Id.* at 68,675.
[14] *Id.*
[15] *Id.* at 38,091.

64,427 small businesses in fiscal year 2010, so this rule will impact approximately 48,965 small businesses.[16]

TCP believes that the purpose and substance of the NPRM is contrary to the intent of E.O. 13556 and the recommendations in *Reining in Excessive Secrecy*. The rulemaking appears to be an attempt to circumvent the new CUI process, in that implementation of this rule would create a regulation which DoD could later reference as authority for a proposed CUI category. Also, the language of many of the substantive provisions of the NPRM seems to go beyond safeguarding toward treating this information as if it were classified. For these reasons, TCP opposes the implementation of the proposed rule in its current form.

The NPRM is an End Run Around the CUI Process Established by E.O. 13556

E.O. 13556 designates the National Archives and Records Administration (NARA) as the Executive Agent to implement the order and oversee agency compliance actions.[17] Pursuant to the order, NARA issued an *Initial Implementation Guidance for Executive Order 13556* ("Guidance") on June 9, 2011, which outlined the steps that agency heads must take to comply with the new CUI framework.[18] E.O. 13556 specifies that agencies are to review all current CUI categories, subcategories, and markings and to submit to NARA only those categories that are authorized pursuant to law, regulation, or Government-wide policy, along with a definition of the category.[19] After reviewing agency submissions, the Guidance requires NARA to publish a list of approved CUI categories in the CUI registry available on the NARA website.[20] Agencies are expected to mark and safeguard CUI information according to registry instructions, and to provide education and training to their personnel to ensure compliance with the new CUI process.[21] Going forward, CUI markings will replace all legacy markings, and only documents that meet the new standards—including documents marked under the old system that are still in use—should be marked and safeguarded as CUI.[22]

Many of the classes of documents listed in DoD's NPRM do not currently require safeguarding or dissemination controls pursuant to law, regulation, or Government-wide policy.[23] That means that under E.O. 13556 and the Guidance, these categories of documents would not qualify for CUI designation under the process described above.[24] DoD's proposed

[16]*Id.*
[17]Exec. Order No. 13,556, *supra* note 3, at 68,675.
[18]NAT'L ARCHIVES & RECORDS ADMIN., CUI OFFICE NOTICE 2011-01: INITIAL IMPLEMENTATION GUIDANCE FOR EXECUTIVE ORDER 13556 (2011) [hereinafter NARA GUIDANCE].
[19]Exec. Order No. 13,556, *supra* note 3, at 68,675.
[20]NARA GUIDANCE, *supra* note 18, at 2.
[21]*Id.* at 2-5.
[22]*Id.* at 3.
[23]For example, "DoD information"—identified in the NPRM as requiring basic safeguarding— and enhanced safeguarding categories such as Critical Program Information and Critical Information fail to qualify as categories of information deserving CUI safeguards by the standards laid out in the Executive Order. The NPRM cites DoD Instructions and Directives as the motivating authority for basic and enhanced safeguarding, but Instructions and Directives are not laws, regulations, or Government-wide policies, nor do they reference those critical categories therein. *See* NPRM, *supra* note 1, at 38,090, 38,092.
[24]*See supra* note 14 and accompanying text.

rule appears to be an attempt to make those documents eligible for CUI designation. If the proposed rule is adopted, it would qualify as a regulation that could later be cited by DoD as a "law, regulation, or Government-wide policy" that would justify CUI designation for the classes of documents listed therein. This type of move is an end run around the new CUI process and is contrary to the intent of the Executive Order and Guidance.

Instead of manipulating the system, DoD should follow the process outlined in the Executive Order and Guidance. This process requires the DoD to submit proposed CUI categories to NARA within 180 days of the date of the Executive Order, along with definitions for each proposed category and the *existing* basis in law, regulation, or Government-wide policy for safeguarding or dissemination controls.[25]

It is possible that an agency might identify a category of unclassified information that truly requires safeguarding, but is not currently protected by law, regulation, or Government-wide policy as required by E.O. 13556. If an agency were to face this situation, it might be appropriate to conduct a rulemaking to develop a targeted regulation to safeguard that category of information. In such a case, however, this class of information should be clearly described in the Federal Register, and the reasons justifying the new regulation and the need for safeguarding the information should be clearly explained. In the current NPRM, however, the classes of information not currently protected by law, regulation, or Government-wide policy are mentioned by name only and the NPRM does not include a precise definition of what kinds of documents those classes of information contain. Instead, readers are directed to visit specified webpages containing PDF documents of lengthy and technical DoD Instructions or Directives from which readers must discern the scope of these categories on their own.[26]

For example, Critical Program Information (CPI)—a category of information not currently authorized by law, regulation, or Government-wide policy for safeguarding and dissemination controls—is listed in the NRPM as a class of information requiring enhanced safeguarding.[27] However, CPI is never explicitly defined in the NPRM and the reasons justifying enhanced safeguarding treatment are not explained. A web address directs the reader to DoD Instruction 5200.39 which discusses CPI, but this document is long and technical and does not provide a practical definition of how to determine which documents fall into this category.[28] Moreover, the web address is provided in the "background" section of the NPRM, but is not included in the language of the proposed amendment to the DFARS which will presumably be incorporated into subsequent contracts involving this type of information.[29] Without a clear definition of CPI at their disposal, government officials and contractors will likely err on the side of caution and generously implement enhanced safeguarding controls to any

---

[25]Exec. Order No. 13556, *supra* note 3, at 68,675.

[26]NPRM, *supra* note 1, at 38,090. As internal DoD policies, these Directives and Instructions have never been subject to public comment or regulatory review.

[27]NPRM, *supra* note 1, at 38,093.

[28]NPRM, *supra* note 1, at 38,090. DoD Instruction 5200.39 is 20 pages long and references no fewer than 29 other DoD Instructions and Directives and authority. None of these documents explain or justify why this category of information requires enhanced safeguarding. *See* DEPT. OF DEFENSE, DOD INSTRUCTION 5200.39, CRITICAL PROGRAM INFORMATION (CPI) PROTECTION WITHIN THE DEPARTMENT OF DEFENSE (2008), *available at* http://www.dtic.mil/whs/directives/corres/pdf/520039p.pdf.

[29]NPRM, *supra* note 1, at 38,090, 38,093.

documents that *might* qualify as CPI to ensure that they comply with the terms of the DFARS. This is an ineffective and unacceptable way for an agency to define and communicate categories of information requiring safeguarding and dissemination controls.

To the extent that DoD is seeking to safeguard information already protected from disclosure by statute, this regulation is unnecessary.[30] Thus, it is unnecessary for DoD to list in the NPRM information protected pursuant to the Privacy Act and the Health Insurance Portability and Accountability Act. DoD can simply submit these categories for approval based on existing statutes.

The Categories of Information Identified for Safeguarding in the NPRM Are Inappropriate for CUI

In addition to the objectionable posturing of the DoD rulemaking, the substantive provisions contained therein are contrary to the intent of E.O. 13556. The Executive Order and Guidance clearly set forth a policy favoring openness and information sharing among agencies and branches of government. The Executive Order states, "This order establishes a program for managing this information . . . that emphasizes the openness and uniformity of Government-wide practice."[31]

The NPRM, on the other hand, reverses this presumption of openness in favor of a presumption of non-disclosure. This is most glaringly reflected in the definitions of "DoD Information," "Government Information," and "nonpublic information" provided in the NPRM, which essentially provide that any information that has not already been disseminated to the public or has not been pre-approved for public disclosure is subject to basic safeguarding controls.[32] This creates a presumption of secrecy in that documents are presumed to be CUI material if not specifically designated otherwise, which is exactly opposite to the stated goals of the Executive Order. In addition, the definition of "nonpublic information" indicates that Freedom of Information Act (FOIA) exemptions would be subject to basic safeguarding measures,[33] despite the fact that E.O. 13556 and the Guidance clearly state that CUI

[30] A statute is a valid form of authority qualifying documents for CUI safeguarding. *See* Exec. Order 13,556, *supra* note 3, at 68,675.
[31] *Id.* at 68,675.
[32] "DoD information" is defined in the NPRM as "any nonpublic information that (1) has not been cleared for public release in accordance with DoD Directive 5230.09, Clearance of DoD Information for Public Release; and (2) is (i) provided by or on behalf of the Department of Defense (DoD) to the Contractor or its subcontractor(s); or (ii) collected, developed, received, transmitted, used, or stored by the Contractor or its subcontractor(s) in support of an official DoD activity." NPRM, *supra* note 1, at 38,092. "Nonpublic information" is defined as "any Government or third-party information that (1) is exempt from disclosure under the Freedom of Information Act (5 U.S.C. 552) or otherwise protected from disclosure by statute, executive order, or regulation; or (2) has not been disseminated to the general public, and the Government has not yet determined whether the information can or will be made available to the public." *Id.* "Government information" is defined as "any unclassified nonpublic information that is (1) provided by or on behalf of the Government to the contractor or its subcontractor(s); or (2) collected, developed, received, maintained, disseminated, transmitted, used, or stored by the Contractor or its subcontractor(s) in support of an official Government activity." *Id.*
[33] *Id.* ("Nonpublic information means any Government or third-party information that is exempt from disclosure under the Freedom of Information Act.")

determinations should be made separate and apart from assessments of FOIA exemptions or any other nondisclosure decisions.[34]

Perhaps the most alarming aspect of the NPRM, however, is that it seeks to extend and grandfather in earlier CUI categories by automatically designating all documents with old CUI markings as deserving of enhanced safeguarding treatment.[35] DoD inserts these old CUI markings, such as "For Official Use Only" and "Sensitive But Unclassified," into the NPRM no less than five times, making it clear that not only do these prior markings qualify these documents for enhanced safeguarding under the proposed rule, but also that contractors would still be responsible for providing any additional safeguarding mandated by those earlier designations.[36] This completely undermines the intent of the Executive Order and Guidance which strictly limit CUI designation and treatment to documents that qualify under the new rules, regardless of prior markings.[37] The Guidance states the need for careful marking of legacy material even more clearly: "The appropriate CUI marking shall be applied [to legacy material] only if the information meets the requirements for designation as CUI."[38] Instead, the DoD seeks to circumvent the review process and inhibit information sharing by automatically incorporating all legacy material into the NPRM which will later serve as the "authority" pursuant to which the DoD supports its proposed CUI categories. The "For Official Use Only" and "Sensitive But Unclassified" markings, in particular, were applied generously in the past, and a rule that automatically converts these documents into CUI would affect a huge amount of material.

The Safeguarding Procedures Detailed in the NPRM Are Inappropriate for CUI

In addition, some of the specific safeguarding requirements detailed in the NPRM at both the basic and enhanced levels are similar to safeguards typically used for classified documents, which is inappropriate in a CUI setting. By definition, CUI material is *un*classified. Nevertheless, the NPRM specifies that contractors should only distribute unclassified DoD Information to subcontractors or employees inside the Contractor's organization on a "need-to-know" basis.[39] The NPRM also requires that information provided from contractors to the Government should only be shared outside of DoD with authorized entities on a need-to-know

[34]*See* Exec. Order 13,556, *supra* note 3, at 68,675. Moreover, the Guidance explicitly states that "the mere fact that information is designated as CUI shall not have a bearing on determinations pursuant to the Freedom of Information Act (FOIA) or any law requiring the disclosure of information." NARA GUIDANCE, *supra* note 18, at 4. *See also* CUI TASK FORCE REPORT, *supra* note 10, at 16.

[35]NPRM, *supra* note 1, at 38,093 (stating that all documents "bearing current and prior designations indicating controlled access and dissemination" are subject to enhanced safeguarding under the NPRM).

[36]*See* NPRM, *supra* note 1, at 38090, 38092-95. Old CUI markings are also grandfathered into the NPRM in reference to reporting requirements. *Id.* at 38,094.

[37]Exec. Order 13,556, *supra* note 3, at 68,675 (specifically requiring agencies to review all categories under the old system and submit to NARA a catalogue of proposed categories under the new system which "shall provide definitions for each proposed category and subcategory and identify the basis in law, regulation, or Government-wide policy for safeguarding or dissemination controls").

[38]NARA GUIDANCE, *supra* note 18, at 3.

[39]NPRM, *supra* note 1, at 38092, 38093.

basis.[40] "Need-to-know" language is traditionally associated with the treatment of classified documents,[41] and importing such language into the CUI context frustrates information sharing.

The NPRM also requires physical or electronic barriers to protect DoD Information, even at the *basic* safeguarding level, with no explanation or justification as to why this would be necessary.[42] The NPRM specifies that when DoD information is not under direct individual control, at least one physical or electronic barrier such as a locked container or room, or login and password are necessary to comply with basic safeguarding procedures.[43] Physical safeguards are traditionally used for classified documents and DoD has not demonstrated any reason why it might be appropriate for them to be incorporated into the CUI framework.[44]

Also troubling are the open-ended provisions included within the basic and enhanced safeguarding requirement descriptions. The NPRM provides that the contractor shall provide "adequate security" to safeguard unclassified information, which is defined as protective measures "commensurate" with the risk.[45] The level of risk and necessity of implementing additional safeguards are left entirely to the contractor's discretion. Also, section (b)(ii) of the enhanced safeguarding portion of the NPRM provides that "the Contractor shall apply *other* information security requirements when the Contractor reasonably determines that information security measures, *in addition* to those identified in those identified [in the basic and enhanced safeguarding sections] . . ., may be required to provide adequate security" (emphasis added).[46] Again, no guidance is provided to contractors on how to determine the necessity and extent of additional safeguards. E.O. 13556 does not contemplate a CUI system based on discretion; quite to the contrary, E.O. 13556 explicitly shunned the "ad hoc" policies and markings of the old CUI system that "led to unclear or unnecessarily restrictive dissemination policies."[47] If adopted, DoD's proposed rule would surely perpetuate the worst qualities of the old CUI system.

Conclusion

The DoD NPRM is not consistent with the goals of the new CUI program and constitutes an end run around the CUI registry process. TCP requests that DoD not adopt this proposed rule and instead comply with the process outlined in E.O. 13556 and the Guidance for obtaining approval of new CUI categories. Through E.O. 13556, the President has initiated desperately needed reforms to create an open, uniform system of CUI to promote information sharing

---

[40] *Id.* at 38095.
[41] ASSISTANT SEC'Y OF DEF. FOR COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE, DEP'T OF DEF., DOD GUIDE TO MARKING CLASSIFIED DOCUMENTS 4, 28 (1997), *available at* http://www.dtic.mil/dtic/pdf/customer/STINFOdata/DoD5200_1ph.pdf.
[42] NPRM, *supra* note 1, at 38093.
[43] *Id.*
[44] *See* U.S. GEOLOGICAL SURVEY ADMIN. DIV., NATIONAL SECURITY INFORMATION HANDBOOK, 440-3-H chpt. 8 ("Whenever classified information is not under the personal control and observation of a cleared person, it must be guarded by cleared personnel or stored in a locked security container . . . When not in use, Top Secret information must be stored in either a GSA-approved security container or vault."), *available at* http://www.usgs.gov/usgs-manual/handbook/hb/440-3-h.html#chapter8.
[45] NPRM, *supra* note 1, at 38,092.
[46] *Id.* at 38093.
[47] Exec. Order 13,556, *supra* note 3, at 68,675.

without compromising security. TCP urges that DoD cooperate in achieving this laudable goal by not adopting its proposed rule.

Sharon Bradford Franklin
Senior Counsel
The Constitution Project
1200 18th Street, NW
Suite 1000
Washington, DC 20036
202-580-6928