RAND CORPORATION

DEBRA SCHROEDER
VICE PRESIDENT, GENERAL COUNSEL,
AND CORPORATE SECRETARY

1776 MAIN STREET
P.O. BOX 2138
SANTA MONICA, CA
90407-2138

TEL 310.451.6983
FAX 310.260.8169
debra_schroeder@rand.org

March 23, 2017

Department of Homeland Security
Office of the Chief Procurement Officer
Acquisition Policy and Legislation
ATTN: Shaundra Duggans
245 Murray Dr., Bldg. 410
Washington, DC 20528

RE: HSAR Case 2015-001

Dear Ms. Duggans:

Thank you for the opportunity to comment on the Department of Homeland Security's (DHS) proposal to amend the Homeland Security Acquisition Regulation (HSAR) to implement adequate security and privacy measures to safeguard Controlled Unclassified Information (CUI) and to facilitate improved incident reporting to DHS.

The RAND Corporation (RAND) shares the Department's commitment to protecting CUI and appreciates the Department's effort to clarify existing rules and contact clauses. However, we are concerned that certain provisions in the proposed rule are inconsistent with the Federal-wide standards for protection of CUI in non-Federal information systems. Of most concern are the provisions that mandate that all DHS contractors comply with various DHS policies and procedures. Some of those DHS policies impose security standards on contractor information systems that are impermissible under the Final Rule on the protection of CUI promulgated by the National Archives and Records Administration (NARA), 32 CFR Part 2002.[1] Our comments below detail our concerns.

RAND is a nonprofit institution that helps improve policy and decisionmaking through research and analysis. We develop solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. Our research spans the issues that matter most, such as security, health, education, justice, the environment, sustainability, development, and international and military affairs. As a nonpartisan organization, RAND is widely respected for operating independent of political and commercial pressures. Quality and objectivity are our two core values.

RESEARCH AREAS
Children and Families
Education and the Arts
Energy and Environment
Health and Health Care
Infrastructure and Transportation
International Affairs
Law and Business
National Security
Population and Aging
Public Safety
Science and Technology
Terrorism and Homeland Security

OFFICES
Santa Monica, CA
Washington, DC
Pittsburgh, PA
New Orleans, LA
Boston, MA
Cambridge, UK
Brussels, BE
Canberra, AU

[1] The NARA Final Rule, entitled Controlled Unclassified Information, 32 CFR Part 2002, went into effect on November 14, 2016. It implements Executive Order 13556, Controlled Unclassified Information, 3 CFR, 2011 Comp., p. 267 (November 4, 2010).

DHS faces complex challenges in preventing terrorism, managing U.S. borders, enforcing and administering immigration laws, safeguarding cyberspace, and strengthening national preparedness and resilience. To help address these challenges, RAND operates the Homeland Security Operational Analysis Center (HSOAC) Federally Funded Research and Development Center (FFRDC) for DHS.

FFRDCs are independent entities that assist the United States government with scientific research, analysis, and development. FFRDCs address critical, long-term problems of considerable complexity; provide immediate, short-term assistance for urgent, high-priority issues; analyze technical questions with a high degree of objectivity; and provide creative and cost-effective solutions to government problems. Working in the public interest, FFRDCs operate as long-term strategic partners with their sponsoring government agencies.[2] In addition to the HSOAC, RAND operates three FFRDCs sponsored by the Department of Defense.

Comment 1

DHS should limit the applicability of the proposed rule to contractors that operate Federal information systems "on behalf of" DHS and should develop a separate rule and alternative contract clause applicable to contractors that handle or use CUI "only incidental to" providing products or services to the Department.

Executive Order 13556, Controlled Unclassified Information "establishes an open and uniform program for managing information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding information that is classified under Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended." Executive Order 13556, Section 1, Purpose (Fed. Reg. Vol. 75, No. 216, p. 68675 (November 9, 2010)). The NARA Final Rule on CUI "standardizes the way the executive branch handles information that requires protection under laws, regulations, or Government-wide policies, but that does not qualify as classified under Executive Order 13526[.]" 32 CFR § 2002.1(b). It standardizes CUI safeguards for both Executive branch agencies and for non-Federal entities, including contractors. The NARA Final Rule's delineation of the universe of information that falls within the definition of CUI is both explicit and expansive: "All unclassified information throughout the executive branch that requires any kind of safeguarding or dissemination control is CUI." Id. § 2002.12(a).

[2] See 48 CFR 35.017, Federally Funded Research and Development Centers.

The NARA Final Rule establishes a clear framework for determining the appropriate safeguarding standards that must be applied to CUI consistently across all Executive branch agencies. The National Institutes of Standards and Technology (NIST) Special Publication 800–171, Protecting Controlled Unclassified Information in Nonfederal Information Systems (hereinafter, NIST 800-171 standard) is the only standard that applies to CUI that is maintained, handled, or used on a contractor's information system "only incidental to" providing products or services to the Government. ("Agencies must use NIST SP 800–171 when establishing security requirements to protect CUI's confidentiality on non-Federal information systems[.]" 32 CFR § 2002.14(h)(2)).[3] An agency is permitted to impose different safeguarding standards – including agency-specific safeguards such as those found in DHS Sensitive Systems Policy Directive 4300A – only if a contractor is operating a Federal information system "on behalf of" the government. ("Information systems that a non-executive branch entity operates on behalf of an agency are subject to the requirements of this part as though they are the agency's systems, and agencies may require these systems to meet additional requirements the agency sets for its own internal systems." 32 CFR § 2002.14(h)(2)).

Under the NARA Final Rule, to determine the appropriate standards and controls for safeguarding CUI that apply to a government contractor, an analysis must be made of the purpose of the contract, which in turn determines the reason that the contractor is collecting, maintaining, or using government information or data. The determining factor is whether the non-government entity/contractor is managing an information system "on behalf of" an executive branch agency, or whether the contractor is using government information "only incidental to providing a service or product" to the agency. The CUI Program regulation 2002.14(h) states:

> Information systems that process, store, or transmit CUI are of two different types:
>
> (1) A Federal information system is an information system used or operated by an agency or by a contractor of an agency or other organization **on behalf of** an agency. An information system operated on behalf of an agency provides information processing services to the agency that the Government might otherwise perform itself but has decided to outsource. . . . Information systems that a non-executive branch entity operates on behalf of an agency are subject to the

[3] DHS acknowledges in footnote 5 on page 6431 of the Federal Register Notice that the NIST 800-171 standard is the appropriate standard for protecting the confidentiality of CUI on non-Federal information systems.

> requirements of this part as though they are the agency's systems, and agencies may require these systems to meet additional requirements the agency sets for its own internal systems.
>
> (2) A non-Federal information system is any information system that does not meet the criteria for a Federal information system. Agencies may not treat non-Federal information systems as though they are agency systems, so agencies cannot require that nonexecutive branch entities protect these systems in the same manner that the agencies might protect their own information systems. When a nonexecutive branch entity receives Federal information **only incidental to** providing a service or product to the Government other than processing services, its information systems are not considered Federal information systems. NIST SP 800–171 (incorporated by reference, see § 2002.2) defines the requirements necessary to protect CUI Basic on non-Federal information systems in accordance with the requirements of this part. Agencies must use NIST SP 800–171 when establishing security requirements to protect CUI's confidentiality on non-Federal information systems (unless the authorizing law, regulation, or Government-wide policy listed in the CUI Registry for the CUI category or subcategory of the information involved prescribes specific safeguarding requirements for protecting the information's confidentiality, or unless an agreement establishes requirements to protect CUI Basic at higher than moderate confidentiality).

32 CFR § 2002.14(h) (emphasis added).

The NARA Final Rule defines the term "on behalf of" an agency as follow:

> (hh) On behalf of an agency occurs when a non-executive branch entity uses or operates an information system or maintains or collects information for the purpose of processing, storing, or transmitting Federal information, and those activities are not incidental to providing a service or product to the Government.

32 CFR § 2002.4(hh).

The rule proposed by DHS does not distinguish between information security standards applicable to non-Federal contractor information systems versus those applicable to Federal information systems. Section 3004.470-3(a) of the proposed rule states that it applies to "any situation where contractor employees may have access to CUI."

(Emphasis added.) Contracting officers are instructed to include the clause at 48 CFR 3052.204-7X whenever contractor employees "will have access to CUI." 3004.470-4(b)(1) (emphasis added). As discussed in more detail in Comment 2 below, both of these sections incorporate by reference several DHS policies and procedures listed on DHS's website, without regard to whether a contractor is operating an information system "on behalf of DHS" or whether a contractor's access to CUI is "only incidental to" providing a product or service to DHS.

Despite the clear distinction mandated by the NARA Final Rule, the DHS proposed rule subjects all contractor access to CUI and all contractor information systems to the same agency-specific policies and procedures and does not apply the NIST 800-171 standard in any situation. The NIST 800-171 standard merits only the most cursory mention in DHS's Federal Register notice: it is mentioned, and promptly dismissed, in footnote 5 on page 6431. Although footnote 5 states that "the information system security requirements in this proposed rulemaking are focused on Federal information systems, which include contractor information systems operating on behalf of an agency[,]" the scope of the proposed rule, and in particular, section 3004.470-3(a) and contract clause 3004.470-4(b)(1), broadly encompasses all circumstances in which a contractor has access to CUI and in which a contractor's information system collects or stores CUI.

As discussed in detail in comments 2, 3, 4, and 5 below, several of the provisions in the proposed rule exceed DHS's authority – as constrained by Executive Order 13556 and the NARA Final Rule – to impose information standards on non-Federal information systems. We propose that DHS remedy these problems with the scope of the proposed regulation in one of the two following ways:

> (1) By explicitly limiting the scope and applicability of the proposed rule as currently written only to contractors that operate a Federal information system "on behalf" of DHS (consistent with the scope described in footnote 5 of the DHS Federal Register Notice) and promulgating a separate rule applicable to non-Federal information systems; or
>
> (2) By modifying the proposed rule to restrict the overly broad language in section 3004.470-3(a) and contract clause 3004.470-4(b)(1) and explicitly apply the NIST 800-171 standard to all non-Federal information systems.

Comment 2

The incorporation by reference of DHS policies into section 3004.470-3 of the proposed rule and in proposed contract clause 3052.204-7X(b)(1) violates Federal-wide policy as to contractors that do not operate Federal information systems.

Section 3004.470-3 of the proposed regulation "requires that CUI be safeguarded wherever such information resides" and includes both "contractor-owned and/or operated information systems operating on behalf of the agency" as well as "any situation where contractor and/or subcontractor employees may have access to CUI." (Emphasis added.) It then includes a blanket mandate that **all** DHS contractors must comply with **all** of the Department's policies and procedures that address safeguarding CUI that are listed at https://www.dhs.gov/dhs-security-and-training-requirements-contractors.

Contracting officers are required to insert the proposed clause at 48 CFR 3052.204-7X in all solicitations and contracts "where [c]ontractor and/or subcontractor employee will have access to CUI[.]" 3004.470-4(b)(1). Proposed contract clause 3052.204-7x(b)(1) requires that contractors provide "adequate security to protect CUI" and states that "[a]dequate security includes compliance with DHS policies and procedures in effect at the time of contract award. These policies and procedures are accessible at https://www.dhs.gov/dhs-security-and-training-requirements-contractors."

The effect of these provisions is that the policies and procedures listed on DHS's website are incorporated by reference both into the regulation and into contracts. Compliance with those policies and procedures is thus both a regulatory and a contractual obligation for all DHS contractors that have access to CUI and to all contractor information systems, without consideration of whether a contractor operates a Federal information system "on behalf of" DHS or whether a contractor receives Federal information "only incidental to" providing a service or product to the Government.

At least one of the departmental policies included in the referenced list – DHS Sensitive Systems Policy Directive 4300A, Version 12.01, February 12, 2016 (hereinafter, DHS 4300A standard) – imposes information security requirements that DHS has promulgated for its own internal systems. This agency-specific standard exceeds the information security requirements set forth in the NIST 800-171 standard.

Executive Order 13556 is specifically aimed at eliminating inconsistent, inefficient, ad hoc agency-specific policies and procedures for managing and safeguarding CUI:

> At present, executive departments and agencies (agencies) employ ad hoc, agency-specific policies, procedures, and markings to safeguard and control this information, such as information that involves privacy, security, proprietary business interests, and law enforcement investigations. This inefficient, confusing patchwork has resulted in inconsistent marking and safeguarding of documents, led to unclear or unnecessarily restrictive dissemination policies, and created impediments to authorized information sharing. The fact that these agency-specific policies are often hidden from public view has only aggravated these issues.
>
> To address these problems, this order establishes a program for managing this information, hereinafter described as Controlled Unclassified Information, that emphasizes the openness and uniformity of Government-wide practice.

Executive Order 13556, Section 1, Purpose (Fed. Reg. Vol. 75, No. 216, p. 68675 (November 9, 2010)).

Consistent with the Executive Order, the NARA Final Rule explicitly limits the authority of agencies to impose agency-specific policies. Agencies "cannot require that nonexecutive branch entities protect these [non-Federal information] systems in the same manner that the agencies might protect their own information systems." 32 CFR § 2002.14(h)(2). Agencies "may not implement safeguarding or dissemination controls for any unclassified information other than those controls consistent with the CUI Program[.]" 32 CFR § 2002.1(c). The NARA Final Rule "overrides agency-specific or ad hoc requirements when they conflict." 32 CFR § 2002.1(i). "Agencies may not implement safeguarding or dissemination controls for any unclassified information other than those controls permitted by the CUI Program." 32 CFR § 2002.12(a).

As set forth in detail in Comment 1 above, the NARA Final Rule stipulates that the NIST 800-171 standard is the only information security standard that may be applied to contractor information systems and contractor employees who maintain, handle, or use CUI "only incidental to" providing a product or service to DHS. 32 CFR § 2002.14(h)(2). Section 3004.470-3 of the proposed DHS rule and corresponding contract clause 3052.204-7X (b)(1) improperly subject all contractors and all contractor information systems to DHS agency-specific standards. These provisions impose agency-specific standards – including the DHS 4300A standard – in "any situation where contractor employees may have access to CUI" (Section 3004.470-3(a))(emphasis added) and whenever contractor employees "will have access to CUI." 3004.470-4(b)(1)

(emphasis added). Under the NARA Final Rule, these DHS 4300A standards cannot be imposed on contractors that handle or use DHS CUI "only incidental to" providing a service or product to DHS. The proposed rule clearly exceeds DHS's authority as constrained by Executive Order 13556 and the NARA Final Rule. 32 CFR §§ 2002.14(h)(1) and (2).

Comment 3

To avoid ambiguity, confusion, and inconsistent contract administration, the term "on behalf of" should be defined in the proposed regulation, consistent with the definition of the term in the NARA Final Rule on CUI.

The term "on behalf of" is used throughout both the NARA Final Rule on CUI and in the proposed DHS regulation. It is a critical term, because it clarifies when an information system is considered a Federal information system that is operated by a contractor, as opposed to a non-Federal contractor information system that merely stores or handles CUI only incidental to providing a product or service to the Government.

For example, the determination of whether proposed clause 3052.204-7X(c), Authority to Operate, should be included in a contract or whether it is "self-deleting" depends on a determination of whether a contractor information system is operating "on behalf of" the agency. Absent a definition of this key term, contracting officers are likely to interpret the applicability of the clause differently, leading to inconsistent standards for protection of information.

The NARA Final Rule includes a definition of the term, and to ensure consistency with the Federal-wide standard, the same definition also should be included in the DHS regulation, as follows:

> (hh) On behalf of an agency occurs when a non-executive branch entity uses or operates an information system or maintains or collects information for the purpose of processing, storing, or transmitting Federal information, and those activities are not incidental to providing a service or product to the Government.

32 CFR § 2002.4(hh).

Comment 4

DHS should add a provision to the proposed rule – and a corresponding contract clause – explicitly specifying that the NIST 800-171 standard must be applied to non-Federal contractor information systems and to contractor employees who handle or use CUI "only incidental to" providing a service or product to DHS.

As discussed in Comment 1, the NARA Final Rule stipulates that NIST 800-171 is the only standard that applies to CUI that is maintained, handled, or used on a contractor's information system "only incidental to" providing products or services to the Government: "Agencies must use NIST SP 800–171 when establishing security requirements to protect CUI's confidentiality on non-Federal information systems[.]" 32 CFR § 2002.14(h)(2). To avoid ambiguity or inconsistency in the application of information security standards, the NIST 800-171 standard should be cited in all instances in which it applies in the DHS regulation – that is, in all situations in which a contractor's information system or contractor employees are handling or using CUI "only incidental to" providing a product or service to DHS.

Comment 5

Some of the categories or subcategories of CUI defined in the proposed regulation are not included the CUI Registry.

The DHS proposed rule includes in its definition of Controlled Unclassified Information some categories of information designated as CUI that are not listed in the CUI Registry. See 3052.204-7X, proposed definition of Controlled Unclassified Information.

The NARA Final Rule establishes the CUI Registry as the "authoritative central repository for all guidance, policy, instructions, and information on CUI (other than [Executive Order 13556] and [the NARA Final Rule])." 32 CFR § 2002.10(a). See also, Executive Order 13556 ("The CUI categories and subcategories shall serve as exclusive designations for identifying unclassified information throughout the executive branch that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies." Executive Order 13556, Section 2, Controlled Unclassified Information (Fed. Reg. Vol. 75, No. 216, p. 68675 (November 9, 2010)).

Agencies do not have the authority to designate categories or subcategories of information as CUI except through the CUI Registry: "CUI categories and subcategories

[set forth in the CUI Registry] are the exclusive designations for identifying unclassified information that a law, regulation, or Government-wide policy requires or permits agencies to handle by means of safeguarding or dissemination controls." 32 CFR § 2002.12(a). "Agencies may use only those categories or subcategories approved by the CUI EA and published in the CUI Registry to designate information as CUI." Id. § 2002.12(b).

The definition of Homeland Security Agreement Information in the proposed DHS regulation is particularly problematic, because it includes within the definition of CUI "information that DHS received pursuant to an agreement with state, local, tribal, territorial, and private sector partners that is required to be protected by that agreement." This definition is vague and overly broad, and does not comport with the definition of CUI set forth in the NARA Final Rule or with the categories or subcategories of CUI included in the CUI Registry.

Comment 6

Proposed Clauses 3052.204-7X(d) (Incident Reporting), 3052.204-7X(e) (Incident Response), and 3052.204-7X(f) (PII and SPII Notification) should be revised to be consistent with the current OMB directive.

In the Discussion and Analysis that accompanies the proposed DHS regulation, DHS notes that "[t]he timing for reporting incidents involving PII or SPII is consistent with OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information." Federal Register Vol. 82, No. 12, p. 6432. The OMB memorandum cited and relied upon by DHS was superseded on January 3, 2017 by OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information. The proposed regulations and contract clauses should be revised to be consistent with the current OMB directive.

Respectfully submitted,

THE RAND Corporation

Debra Schroeder

By Debra L. Schroeder
Vice President, General Counsel, and Corporate Secretary