Via Regulations.gov

Regulations Comments Desk
(External Policy Program, Strategy and Performance Division)
Suite 4100
National Archives and Records Administration
8601 Adelphia Road
College Park, MD 20740-6001


To Whom It May Concern:

On behalf of the American Bar Association (“ABA”) Section of Public Contract Law (“Section”), I am submitting comments on the Proposed Rule cited above. The Section consists of attorneys and associated professionals in private practice, industry, and government service. The Section’s governing Councils and substantive committees include members representing these three segments to ensure that all points of view are considered. By presenting their consensus view, the Section seeks to improve the process of public contracting for needed supplies, services, and public works.

The views expressed herein are presented on behalf of the Section. They have not been approved by the House of Delegates or the Board of Governors of the ABA and, therefore, should not be construed as representing the position of the ABA.

1 Mary Ellen Coster Williams, Section Delegate to the ABA House of Delegates, and Marian Blank Horn, Kristine B. Kassekert, and Heather K. Weiner, members of the Section’s Council, did not participate in the Section’s consideration of these comments and abstained from the voting to approve and send this letter.

2 This letter is available in pdf format at http://www.americanbar.org/groups/public_contract_law/resources/prior_section_comments.html under the topics “Ethics and Compliance.”
I. INTRODUCTION

On January 11, 2017, the Information Security Oversight Office of the National Archives and Records Administration (“NARA”) proposed revising the National Industrial Security Program (“NISP”) Directive. The NISP safeguards classified information the Government or foreign governments release to contractors, licensees, grantees, and certificate holders. This proposed NISP revision adds provisions incorporating executive branch insider threat policy and minimum standards; identifies the Office of the Director of National Intelligence and the Department of Homeland Security as new cognizant security agencies (“CSAs”); and adds responsibilities for all CSAs and non-CSA departments and agencies to reflect oversight functions that are already detailed for private sector entities in the National Industrial Security Program Operating Manual (“NISPOM”). The proposed revisions also make other administrative changes to be consistent with recent revisions to the NISPOM and with updated regulatory language and style.

We have focused our comments on the insider threat provisions and the identification of a number of other areas that we respectfully suggest may benefit from future rulemaking.

II. COMMENTS

A. Comments on the Proposed Rule.

The Section recommends ensuring that the definition of “insiders” in the NISP Directive is consistent with the NISPOM definition and is inclusive of a wide variety of potential threats. That does not currently appear to be the case in the proposed rule.

In Section 2004.4(p) of the proposed rule, insiders are defined as “entity employees” who are “eligible” to access classified information and “may be” “authorized” to access any resource. This could introduce confusion as to when a person becomes eligible versus authorized, as well as when they may access classified information versus when they may access any resource. Furthermore, the use of “entity employees” here is limiting. The scope of insiders should encompass anybody with authorized access to a contractor site, including not just employees, but also individuals working for other contractors/subcontractors, government personnel, visitors, janitors, etc.

The NISPOM at Appendix C provides a more straightforward definition of “insiders,” defining them as: “Cleared contractor personnel with authorized access to any Government or contractor resource, including personnel, facilities, information, equipment, networks, and systems.” This definition, however, like the proposed definition of “entity employees” above, may be too narrowly focused on contractor personnel while omitting the other types of authorized personnel who may be on site.

The Section recommends adopting the following definition of “insiders” based on a slightly-revised version of the pre-existing NISPOM definition: “Cleared personnel with authorized access to any Government or contractor resource, including personnel, facilities, information, equipment, networks, and systems.” Using this language would promote uniformity
and clarity while also covering the types of cleared personnel we believe the rule is intended to be covered in order to comprehensively address the risk of insider threats.

In addition, the Section proposes a clarification to the definition of “insider threat” in Section 2004.4(q) of the proposed rule. The first sentence in this section is a broad statement that threats include any that might harm U.S. national security. The second sentence, however, narrowly focuses only on potential harm to information about the entity or program generally, potentially excluding threats to physical security. Accordingly, the Section recommends that this second sentence be revised as follows to help better illustrate the variety of potential insider-threat targets in a way that benefits all readers: “Insider threats may include harm to put at risk any asset or resource, including entity or program information to the extent that the information impacts the entity's or agency's obligations to protect classified information.”

Moreover, in reviewing Section 2004.24(a)(2) of the proposed rule, it appears that major parts are missing from the NISPOM Change 2 update via industrial security letter (“ISL”) 2016-02, issued on May 21, 2016. Change 2 requires contractors to establish and maintain an insider threat program to detect, deter, and mitigate insider threats. This section also should provide a cross reference to standards regarding the types of conduct that must be reported as adverse information.

The Section recommends revising this section as follows: “Requiring entities to: (i) deter, detect, and mitigate insider threats; and (ii) monitor, gather, integrate, report, and review insider threat program activities and response actions in accordance with 32 C.F.R. § 147, Defense Security Service (DSS) Industrial Security Letter (ISL) 2011-04 and the provisions set forth in the NISPOM (or equivalent).”

B. Additional Areas to Consider for Rulemaking.

The Section has identified additional areas that we recommend NARA consider addressing in a future rulemaking:

- **Expressly allow consultants to provide services to the Government.** Section 2-212 of the NISPOM together with Section 12 of ISL 2006-02 (also discussed at http://www.dss.mil/about_dss/news/20130708.html) define consultants as those who provide professional or technical assistance to the contractors, and limit the provision of such services to one consultant per consulting firm. The definition does not contemplate the provision of services directly to the Government. This seems inconsistent with current industry practice, where consultants are providing services to the Government and many firms have numerous professionals supporting the same client contractor. We recommend revising proposed Section 2004.36(b) to: (i) allow consultants to deliver services directly to the Government on behalf of the contractor; (ii) allow multiple consultants per consulting firm if those services are only provided to the contractor; (iii) allow consulting firms to be owned by individuals who are not the consultant or their immediate family; (iv) allow the contractor to process the foregoing multiple consultants for personal security clearances (“PCLs”) under the contractor’s facility clearance
(“FCL”) and without requiring a subcontract to be issued to the consultant’s firm and without the consultants obtaining their own FCL.

- **Allow consultants to retain their clearances without a prime contract.** Under current rules, consultants are not allowed to retain their clearances unless they are tied to an active prime contract. We recommend considering allowing professional services firms (law firms, accountants, finance, medical, etc.) to obtain and retain their own FCL and associated PCLs, without needing a permanent government contract or subcontract, if they: (i) are initially sponsored by a contractor and receive an FCL; (ii) demonstrate a reasonable likelihood of providing ongoing cleared work as consultants to contractors; and (iii) cover the costs of retaining their FCL and PCL.

- **Better define the “Influence” in Foreign Ownership, Control, or Influence (“FOCI”).** In connection with Sections 2004.34(a)(2)(ii) and (c)(2)(viii) of the proposed rule, the Section recommends clarifying whether FOCI influence includes a foreign entity’s control over supplies, parts or services, and what degree of such control would trigger FOCI.

### III. CONCLUSION

The Section appreciates the opportunity to provide these comments and is available to provide additional information or assistance as you may require.

Sincerely,

![Signature]

James A. Hughes
Chair, Section of Public Contract Law

cc:
Aaron P. Silberman
Kara M. Sacilotto
Linda Maramba
Jennifer L. Dauer
Council Members, Section of Public Contract Law
Chairs and Vice Chairs, Ethics, Compliance and Professional Responsibility Committee
Craig Smith
Samantha S. Lee