Joint COGR/AAU Letter to NIST on Controlled Unclassified Information

Author: COGR and AAU

Published Date: 05/12/2015

May 12, 2015

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930)
Gaithersburg, MD 20899-8930

To Whom It May Concern:

RE: Revised Draft NIST 800-171

On behalf of the Council on Governmental Relations and the Association of American Universities, we appreciate NIST's responsiveness to some of the concerns we expressed in our comment letter of January 16, 2015 on the revised draft guidance concerning controlled unclassified information (CUI) outlined in NIST Special Publication 800-171.

We believe eliminating mention of federally funded basic and applied research as explicitly subject to the requirements and further clarification of the distinction between federal and nonfederal information systems are improvements over the previous draft. We also appreciate that the revised draft 800-171 recognizes that isolating CUI into its own security domain and limiting the security requirements accordingly may be the most cost effective and efficient way for nonfederal organizations to satisfy the security requirements.

However, we urge NIST to strengthen its recognition that nonfederal organizations may implement alternate security measures to satisfy particular requirements. We are concerned that the 800-171 standards will become compliance requirements without a strong emphasis on the need for flexibility in their implementation. As an example, the mapping statements on p. 6 and footnote 19 are helpful but it is unclear how they will be reflected in the actual FAR compliance clause.

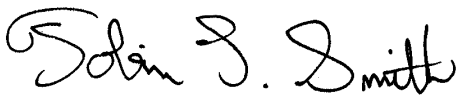
We recognize that NIST does not have compliance responsibilities as stated on p. 2. However, footnote 9 indicates that 800-171 may be referenced in federal contracts until an implementing FAR clause is issued. We reiterate the concern expressed in our previous comments that the 800-171 standards are likely to become prescriptive. As noted previously, 800-171 sets forth a large number of categories and controls, some of which (e.g. multifactor authentication) will be challenging to implement, particularly for large research universities. The IT infrastructure at most universities tends to be highly decentralized. Institutions will have to establish separate segregated business units to comply with these requirements, which will have significant cost and compliance implications for the universities our associations represent. Significant additional personnel and infrastructure resources are likely to be needed.

We recognize the importance of protecting the confidentiality and integrity of CUI. However, policymakers in both the executive and legislative branches are increasingly concerned with the cumulative burden of federal compliance requirements. As stated in our previous comments, the

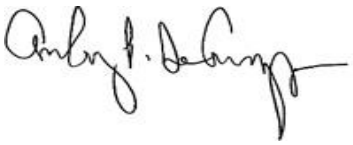
onus needs to be on the federal agency to clearly state in its solicitations and contractual documents when CUI is involved and when the standards must be invoked (as well as that compliance costs associated with the CUI requirements may be included as direct costs). Our biggest fear, based on experience with FISMA requirements, is that the flexibility implied in the NIST guidance will be lost, and the default will be to require full compliance with the 800-171 security requirements in many government contracts. We urge NIST to address these concerns in its final version of Special Publication 800-171.

We appreciate the opportunity to comment and would be happy to engage further with you on any of the points we have raised concerning this matter.

Sincerely,



Tobin L. Smith
Vice President for Policy
Association of American Universities



Anthony P. DeCrappeo
President
Council on Governmental Relations