July 14, 2023

Submitted via email to 800-171comments@list.nist.gov

Mr. Ron Ross
Ms. Victoria Pillitieri
National Institute of Standards and Technology
Computer Security Division / Information Technology Laboratory

Re: NIST SP 800-171 R3 Initial Public Draft

Dear Mr. Ross and Ms. Pillitieri:

This letter is to express the views of The Coalition for Government Procurement ("The Coalition") on the Initial Public Draft (IPD), NIST SP 800-171 Rev. 3 ("Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations"), which NIST published for comment on May 10, 2023. The Coalition offers this narrative letter, with certain observations that concern the publication taken as a whole, as well as a table of specific observations that uses the Comment Template made available by NIST.

By way of background, The Coalition is a non-profit association of firms selling commercial services and products to the Federal Government. Its members collectively account for a significant percentage of the sales generated through General Services Administration contracts, including the Multiple Award Schedule program. Members of The Coalition also are responsible for many of the commercial item solutions purchased annually by the Federal Government. These members include small, medium, and large business concerns. The Coalition is proud to have collaborated with Government officials for 40 years in promoting the mutual goal of common-sense acquisition. The Coalition has over 300 members, 25% of which are small businesses. Many of our businesses have contracts with the U.S. Department of Defense ("DoD") as well as federal civilian agencies.

OVERVIEW COMMENTS

We understand that some of our narrative observations may be outside the responsibilities of NIST or its authorities under Executive Order 13556. SP 800-171, however, is used widely by the Department of Defense and other federal agencies, and it has influence internationally. The IPD for Rev. 3 has many strengths as a document articulating security measures to protect Controlled Unclassified Information (CUI). It increases, however, overall burdens and compliance costs that will affect tens of thousands of private sector entities. Without clear leadership by the Executive Branch, and coordination among federal departments and agencies, Rev. 3 may produce unintended consequences disproportionate to the security improvements it seeks.

- **If a majority of contractors obligated to satisfy Rev. 3 cannot afford or do not understand how to comply, Rev. 3 will not be successful.**

In IPD Rev. 3, NIST has made much progress in explaining why controls are present and how they are to be accomplished. Unfortunately, these accomplishments also cause tens of thousands of companies to face security demands beyond too many already existing that they are struggling to satisfy. NIST is correct that it is not its business to be concerned with how agencies implement SP 800-171 contractually. It is also accurate that, under the referenced Executive Order (EO), and the Federal Information Systems Modernization Act (FISMA), its focus is upon the protection of CUI confidentiality regardless of where, outside federal systems, that CUI ultimately may reside. Separating these propositions from the realities of implementation is hazardous, however. NIST does admirable work, but this standard, in particular, will not exist in a vacuum separated from the business circumstances and capabilities of federal suppliers.

It is ***only*** by terms in a government contract that commercial organizations are obligated to employ NIST SP 800-171. The contractual mechanisms, and how they are administered, matter much. Similarly, new contractual obligations, to be imposed on federal contractors, may require statutory authorization and, ordinarily, come into effect only after rulemaking. The Executive Branch therefore controls the "how," "when," and "upon whom" SP 800-171 Rev. 3 will impact government contractors. Our letter calls for accelerated and increased participation by leaders across the Executive Branch.

- **NIST should increase the involvement of relevant Executive Branch agencies and departments before the issuance of SP 800-171 Rev. 3.**

There is concern that Rev. 3, if finalized in its present IPD form will be costly and prove increasingly difficult for small and medium-sized enterprises (SMEs). Apart from the many companies that will be affected, other stakeholders include the White House (including the Office of Management and Budget (OMB) and the Office of the National Cyber Director (ONCD)), the Small Business Administration (SBA), and the agencies and departments who now do or will require SP 800-171 compliance by contract.[1]

The issuance of Rev. 3 without the involvement of the Executive Branch agencies which set federal cyber policy and the federal agencies and departments who will impose SP 800-171 by contract, neither the "using" agencies nor the "affected" contractors may not be ready, able, or even willing to implement the revised standard.

- **That SP 800-171 IPD Rev. 3 employs so many "organization-defined" parameters makes Executive Branch involvement more urgent and important.**

NIST explains that it produces the SP 800-171 standard for the benefit of the federal agencies whose CUI may end up in private hands. The Coalition believes that the role of NIST should not be "decoupled" from the agencies that will employ it, even if it is not NIST's role to shoulder the needed cyber policy planning and interagency coordination. In the Rev. 3 IPD, there are more than 100 security parameters that are to be "organization-defined." NIST has explained that the "federal government" is the "organization," and reasons that each federal customer conceivably may have its own minimums or objectives for each parameter. That approach is sensible in

[1] It is essential to recognize and act upon distinct risks that SP 800-171 Rev. 3 presents to small businesses. In Senate testimony, on May 18, 2021, a DoD official explained: "Nearly all firms in the third and fourth tiers of the supply chain, or 74% of the defense industrial base, are small businesses according to the Department's contracting data."

theory, however, any individual government contractor may deal with many agencies and many individual customers within that agency. The individual contractor will face different parameters defined by or within different agencies, without advance knowledge of any clear minimum, and with potentially unworkable inconsistencies, This assumes that the various federal agencies will have any idea, when SP 800-171 Rev. 3 becomes effective, *what* parameters each should decide or *which* parameters (if any) should be left to contractor discretion.

We are concerned that large numbers of federal contractors will be negatively impacted, especially SMEs, unless coordination is accomplished now by or on behalf of the agencies that now or will impose SP 800-171 upon their contractors. We appreciate that different agencies, and indeed different requiring activities with individual agencies, may have their own ideas of what "values" to impose as the presently undefined "parameters" in IPD Rev. 3. In order for SP 800-171 Rev. 3 to be implemented effectively, companies need to know, ***before*** SP 800-171 Rev. 3 becomes effective, or at least before it is imposed upon them contractually, initial values and boundaries of these parameters. Companies also need to be informed of the timing of agency implementation.[2]

- **Certain NIST assumptions could face challenges in practical application.**

There is an assumption that each federal department and agency will determine, separately and independently, whether, when and how to use SP 800-171 Rev. 3, and that the controls of Rev. 3 should apply equally to any organization, of any type or size, when they are contractually obligated to protect CUI. The theory is that the protected information does not lose its value, to the national interest, when it is outside the federal environment, and that value doesn't change with the size or business nature of the nonfederal organization which possesses or uses such information.

However, while every federal agency and department has information that constitutes CUI, and such information is shared routinely with contractors, grantees, and other nonfederal partners, it is ***only*** the Department of Defense that today, by contract, requires "adequate security" to protect the confidentiality of CUI using SP 800-171. What this circumstance means, of course, is that most federal agencies have chosen not, or at least not yet, to impose SP 800-171. They may be very wary of the "practical" ramifications of SP 800-171, in its present form (Rev. 2), upon ***their*** suppliers.

Also implied in SP 800-171 IPD Rev. 3, and in DoD's present cyber regulations, is that each or any form of CUI, once so designated or established, merits the same level of protection. In contrast, not all CUI has the same significance to the national interest if its confidentiality is compromised. SP 800-171 IPD Rev. 3 does not set a lower bar for one form of CUI versus another, any more than it offers SMEs a path to compliance that is less costly.

The real world circumstances, limitations, and means of tens of thousands of actual contractors who operate highly varied businesses have practical implications for the aforementioned rationale. Although they may be outside NIST's authority, they ***are*** the problem of the White

[2] The DoD clause, DFARS 252.204-7012, calls upon contractors to use the version of SP 800-171 "in effect at the time the solicitation is issued or as authorized by the Contracting Officer." A precipitous switch-over from Rev. 2 to Rev. 3 could be calamitous. DoD can employ a "class deviation" and issue other regulatory guidance to advise companies of what to expect, and when.

House, OMB, ONCD, the SBA, and other federal agencies and departments. This is another reason that a national policy and interagency coordination is needed for the finalization, roll-out, and deployment of SP 800-171 Rev. 3.

- **Greater specificity in the controls of SP 800-171 IPD Rev. 3 can reduce or preclude flexibility in application to individual contractors.**

NIST has acknowledged, in effect, that SP 800-171 Rev. 2 is not very precise in what actions contractors must take to satisfy each of its 110 enumerated requirements. Although NIST recognizes that there are those in the security community who favor this flexibility, it is evident, from IPD Rev. 3, that it has chosen to take the opposite tack, *i.e.*, to make SP 800-171 ***much*** more prescriptive and to remove (or at least greatly narrow), both from organizations seeking to comply, and their future assessors, latitude to choose the lesser cost, but sufficient, solution among a range of compliant possibilities.

This approach is a further reason for early and material involvement from Executive Branch leadership. If there is just one or a narrow range of permissible "answers" to security questions, then it is the responsibility of individual agencies and departments to manage and mitigate the implementation risks for their respective contractor communities. Executive Branch leadership should recognize the very real possibility that some, many, or even most federal agencies will not adopt or implement SP 800-171 Rev. 3 if they conclude that that their suppliers will be unable to meet the compliance demands. Consider FAR Case 2017-016, the "Controlled Unclassified Information (CUI)" rule, which has remained pending for about seven (7) years. See View Rule (reginfo.gov). It is this rule, if and when, promulgated that would apply SP 800-171 to civilian agencies. As noted, only DoD today has regulations, and by contract, it requires its suppliers to use SP 800-171 to protect CUI.

Over time, different implementation strategies may emerge among departments and agencies. Some may, and some may not, impose assessment mechanisms, such as DoD intends, through the CMMC program. Overarching federal coordination, led by White House entities such as OMB and ONCD, could go a long way to producing a logical, coherent, consistent and achievable deployment of SP 800-171 Rev. 3, and to achieving the long-sought consistency in federal cyber regulations.

- **The Executive Branch must consider whether SMEs can close the "business case" to take contracts subject to SP 800-171 Rev. 3.**

Although its leadership acknowledges concerns over the ability of SMEs to satisfy SP 800-171 Rev. 3, NIST does not consider the solution to this problem to be within its ambit. Executive Branch leadership should not lose sight of the fundamental "business case" question that every federal supplier will consider. Congress has shown it is greatly interested in this question. This question is more acute for smaller companies and the many enterprises who provide valuable supplies and services to federal agencies, but whose business is not dominated by government customers. Is there a return on necessary expenditure and commitment of resources? As the expense and other demands of federal CUI protection requirements rise, the business case is harder to close. Money wasted on unnecessary processes can be better spent to achieve and

sustain security where risks are greatest and where the consequences of breach are most significant.[3]

Our specific Comments from individual member companies are included in the attached. The Coalition hopes you find these comments useful and thanks you for your time and consideration. Should you have any questions or concerns, please contact the undersigned at RWaldron@thegp.org or 202-331-0975.

Sincerely,

Roger Waldron
President

[3] "Perfect is the enemy of the good," a phrase attributed to the 18th century writer Voltaire, also has been expressed as the "Pareto principle," which suggests that, for many outcomes, roughly 80% of consequences come from 20% of the causes. For protection of CUI, better outcomes will result from security requirements which recognize different contractor circumstances and accommodate different means of compliance, rather than through insistence upon idealized methods that assume operational equivalence among the enterprises subject to these requirements.