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.

Comment #	Submitted By (Name/ Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
	Coalition for Gov't Procurement						
1	CGP	General	Fundamentals	iii		Eliminating the distinction between "basic" and "derived" requirements may simplify the presentation but it also eliminates the opportunity for agencies to exclude "derived" requirements or to limit them to circumstances where law, policy or governmentwide regulation require.	
2	CGP	General	Fundamentals	iii		We support the update to align more closely to SP 800-53 Rev. 5 and favor further work on the prototype CUI overlay. We are concerned that the "step" from Rev. 2 to Rev. 3 (and further to such an overlay) will have much greater impact upon contractors than is presently recognized.	
3	CGP	General				Clear and Consistent CUI Guidance: NIST should help users understand the differences between 800-171 and other related NIST publications. An example would be the alignment of 800-171 and 800-172. Additional guidance on when which document applies could reduce confusion by DIB participants. Encourage NARA, DoD, and other agencies to clarify and provide additional guidance for contractors.	
4	CGP	General				Alignment of 800-171 to existing NIST documents and federal regulations: Align 800-171 with other procurement-related cybersecurity guidance: Examples include the Department of Defense CMMC 2.0 program and Homeland Security Acquisition Regulation - Safeguarding of Controlled Unclassified Information.	
5	CGP	General	Fundamentals	iv		IPD Rev. 3 reduces the number of former NFO controls and increases the explicit requirements for Policies. We support this change.	
6	CGP	General	Fundamentals	3	57	Federal information designated as CUI may have the same value whether in or outside a federal information sysem, but commercial organizations are not legally bound to protect that CUI except as required by regulation or contract clause	
7	CGP	General	Fundamentals	3	59	This misstates the actual requirement. Only DoD presently imposes by regulation and contract clause an obligation for its suppliers to use SP 800-171 to protect the confidentiality of CUI.	
8	CGP	General	Fundamentals	3	61	The presumption of uniform safeguards tends to "homogenize" contractor information systems without due recognition of the many varieties of actual circumstances and security systems.	
9	CGP	General	Fundamentals	4	77	CGP supports adding the families of Planning, System and Services Acquisition, and Supply Chain Risk Management, but does not believe the IPD provides sufficient information to contractors to implement the requirements for these new families.	
10	CGP	General	Fundamentals	4	79	By our count, there are about 117 instances where a requirement includes an "*organization-defined parameter.* " This means that contractors subject to Rev. 3 will not know who will set such such parameters, when, or what minimum values will be set.	

Comment #	Submitted By (Name/ Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
11	CGP	General				Responsible entity for organization-defined parameters (ODP): Who is ultimately responsible for defining ODPs? Is the NIST intent to allow industry participants to define and manage ODPs based on the risk? Or is the intent the ability of federal agencies and contract officers to define ODPs?	
12	CGP	General	Fundamentals	4	80	NIST doesn't identify or specify the "federal organizations" that will specify values. Presumably, there may be many such organizations that set different values affecting common information systems of individual contractors. This may not be workable.	
13	CGP	General	Fundamentals	4	84	NIST indicates that the parameter values can be "guided and informed by laws, Executive Orders," etc. True. But without active coordination effort by federal authorities, the results will be scattershot.	
14	CGP	General	Fundamentals	4	87	The "discussion section" is said to be "informative, not normative," but CGP is very interested to see if the companion document, SP 800-171A Rev. 2, follows through on this approach. Risks that the Rev. 3 IPD imposes excessive demands upon SMEs can be aggravated by the "density" of what -171A Rev. 2 may demand in assessments.	
15	CGP	General	Requirement 3.1.1	5	116	Requirement 3.1.1 deserves credit for better explanation of the elements of sufficient Account Management. However, it illustrates how much has changed from Rev. 2 and the additional and more costly complexity. Also, in this single requirement there are five values that are "organization defined."	
16	CGP	General	Requirement 3.1.5	7	229	We support the proposition of "Least Privilege" but have concern that many if not a majority of SMEs potentially subject to this rule will it prohibitively expensive to implement this "zero trust" type approach. This illustrates our pervasive concern that requirements, now updated and better explained, have become much more demanding and costly. We support introducing more flexibility in how controls are chosen and implemented.	
17	CGP	General	Requirement 3.1.5	8	232	We understand that least privilege demands organizational policies to enforce through technical means. As written, however, these could be defined not by the commercial enterprise (contractor) but by one, several or many federal "organizations," an approach we do not consider to be workable.	
18	CGP	General	Requirement 3.1.6	8	251	Here again, it is difficult to envision how an organization can implement this requirement (which we support conceptually) where it does not know and must await one or more federal organizations to define the essential parameters without which the requirement cannot be met.	
19	CGP	General	Requirement 3.1.12	11	357	We have no objection to the principles expressed in 3.1.12 a - e, but we wonder why NIST has not considered how this and similar requirements can be satisfied by Managed Service Provides, or other external service providers, who may provide compliant solutions to many clients.	

Comment #	Submitted By (Name/ Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
20	CGP	General	Requirement 3.1.20	13	452	This is one of several requirements with increased importance by reason of changes in work patterns and methods. If one assumes that nearly every organization permits or relies upon use of external systems, how can any organization define and operate "compliant" practices if the essential operating values are "organization-defined" and likely unknown when Rev. 3 becomes effective. As to MSPs and other external service providers, how are they to accommodate the potential differences in organization-defined parameters?	
21	CGP	General	Requirement 3.1.21	14	478	The same problem is present in 3.1.21.b as an organization will know that it is to "[r]estrict the use of organization-controlled portable storage devices" but can only guess how and affecting whom. As a **general proposition**, we propose that NIST state that the commercial organizations may use their reasonable judgment to set any such values until such time as federal entities set controlling and applicable values. This comment applies across all instances where values are "organization-defined."	
22	CGP	General	Family 3.3 (and other	17	602	We appreciate the importance of "Audit and Accountability" for internal awareness of security performance and for incident response and forensics, among other purposese. Here again, the proliferation of "organization-defined" values means that, upon the effectiveness and applicability of Rev. 3, organizations won't and can't know what to do.	
23	CGP	General	Family 3.4 (and other	21	765	Our perspective is that NIST continues to assume that the majority of enterprises subject to these requirements will be individually responsible for satisfaction of requirements within perimeter systems that they define and operate. We submit that the trend is well established that increasing numbers of government contractors seek to rely upon cloud or managed service providers, and to "inherit" compliance that is accomplished by the third party service provider. Configuration Management is such an area. We urge NIST to consider how each of the requirements can or should apply to such service providers. It will serve the common federal and nonfederal purposes to define requirements (and, later, assessment methods) to accommodate if not facilitate accomplishment by such service providers.	
24	CGP	General	Family 3.6	31	1151	We acknowledge that the mission of NIST here is protection of Confidentiality of CUI. However, we think NIST should consider how Rev. 3 can improve both protection against ransomware, as a distinct threat class, and recovery (resilience) should a ransomware attack occur. Under the Incident Response category, we urge NIST to consider how it can improve enteprise policy and process to detect, analyze and report events. In the same family, NIST might improve requirements for governance and speed of response procedures.	

Comment #	Submitted By (Name/ Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
25	CGP	General	Requirement 3.12.4	46	1716	We support the concept of independent assessment, as we recognize the limits of self-attestation. However, the experience with DoD with the CMMC initiative shows just how complex it is to establish credentials for assessment and contractual mechanisms to have those accomplished. Here, a further consideration is what standards or process will govern such assessments, whether there are sufficient number of assessors, and what role federal organizations play in the process, standards, selection of assessors, and after-assessment actions. NIST should clarify that it anticipates internal assessments, within capable organizations, and that it allows enterprises to select independent assessors absent more strictures from federal customers or regulators.	
26	CGP	General				Independent Assessment: NIST should revise the definition of an “independent assessment” such that an organization can define internal controls to support conduct of the assessments by in-house employees.	
27	CGP	General	Requirement 3.13.11	51	1915	Versus 3.1.13 of Rev. 2, we note that "cryptographic protection" now does not require "FIPS-validated cryptography" but intead there may be "organization-defined types of cryptography." As is widely recognized, many companies struggled with FIPS 140-2. It will be difficult to plan, act, or have assurance of compliance when companies do not know what "type" of cryptography or validation will be permitted or required. It is no help to commercial enterprises for NIST to state, as in the Discussion here, that "Cryptography is implemented in accordance with applicable laws, 1921 Executive Orders, directives, regulations, policies, standards, and guidelines.	
28	CGP	General	Family 3.15	56	2126	We support the addition of this Family with its three elements. Without enteprise planning, it is difficult for organizations to have confidence in their security, know how to implement security measures, or evaluate their own security accomplishments. Required planning steps, including the SSP (of course), also are key for potential government evaluation or assessment of compliance.	
29	CGP	General	Requirement 3.16.1	57	2177	We are aware of the great deal of work that NIST has done with respect to systems security engineering, as it is the subject of NIST SP 800-160v1r1 and SP 800-160V2r1, which together (195+310) comprise 505 pages. We question whether it is feasible or prudent to "transpose" from the complexities of 800-160, which are intended for federal information systems, to just one sentence in requirement 3.16.1 ("Apply systems security engineering principles in the specification, design, development, implementation, and modification of the system and system component.") We question whether more than a handful of companies potentially subject to SP 800-171 Rev. 3 will be able to accomplish this requirement, even assuming they know enough from the one sentence to articulate a compliant plan of action.	

Comment #	Submitted By (Name/ Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
30	CGP	General	Requirement 3.16.3	59	2224	As noted, we recognize the importance of External System Services to the plans and actions of many commercial organizations who supply to federal organizations. However, this vitally important subject seems to have received "undertreatment" here and, again, critical parameters are left to be "organization-defined" later. NIST should consider developing an overlay to accompany Rev. 3 which provides more guidance on what is expected on the "client" as well as the "provider" side of external services.	
31	CGP	General				Supply Chain Risk Management section 3.17: NIST should align requirements in 3.17 in the software with NIST SSDF's software supply chain security requirements and provide a mapping as it provided for NIST 800-53.	
32	CGP	General	Family	59	2250	We appreciate the importance of Supply Chain Risk Management and encourage enterprises to adopt the principles of this Family. However, these are new requirements for the thousands of companies already subject to SP 800-171. That there are many choices and complexities is very well demonstrated by NIST SP 800-161 Rev. 1, released in May 2022, a 326-page document. Our concern is that, beyond the concepts, there is not enough in requirements 3.17.1, 3.17.2, and 3.17.3, for most organizations to know what to do. Again, key values for controls are "TBD" since they are "organization-defined." We are concerned about the boundaries of effort and expense that may be required for compliance, especially where simplified statements of complex subjects are likely to complicate the companion assessment requirements of SP 800-171A Rev. 1.	
33	CGP	General				Clarify flow-down of obligations between DIB prime and sub-contractors: NIST should provide additional guidance on what requirements apply at the prime and/or subcontractor level. DIB participants have uncertainty about whether and how prime contractors are expected to ensure subcontractor compliance.	
34	CGP	General				Adherence for existing contracts: Is the new revision applicable for only new contracts? If the revision applies to existing contracts, what it the timeframe for adherence? These are questions which must be addressed by each federal agency intending to apply Rev. 3. DoD, for example, may find it necessary to use a “class deviation” to avoid precipitous imposition of the revised Standard.	
35	CGP	General				Ability of small and medium size DIB organziations to meet requirements: With the DIB made up of hundreds businesses providing technology and professional services to all federal agencies, NIST should consider the impact on of medium and small size businesses and their ability to adopt the 800-171 requirements.	
36	CGP	Editorial	Publication	69	2637	There is no definition of the acronym "NCO."	Please define "NCO."