From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Cc: [redacted]
Subject: [800-171 Comments] RE: The Coalition for Government Procurement"s Comments on SP 800-171 Rev 3
Date: Monday, July 17, 2023 3:23:03 PM
Attachments: CGP-Comments-to-sp800-171r3-ipd Revised Final.xlsx

---

Mr. Ross and Ms. Pillitteri,

We received some revisions to our comments from our members over the weekend and, if possible, would greatly appreciate if you could accept a revised version of the comments we made in the comment template. The cover letter is unchanged.

Thank you for your consideration,
Ian Bell
Policy Analyst
The Coalition for Government Procurement
[redacted]

THE COALITION
FOR GOVERNMENT PROCUREMENT

From: Ian Bell
Sent: Friday, July 14, 2023 4:49 PM
To: 800-171comments@list.nist.gov
[redacted]
Subject: The Coalition for Government Procurement's Comments on SP 800-171 Rev 3

Mr. Ross and Ms. Pillitteri:

Attached are the Coalition for Government Procurement's final comments on the third revision of SP 800-171. We have included both general comments, covering industry concerns regarding SP 800-171 and exogenous conditions NIST should consider as the development of the standard continues (the PDF document), and comments on specific requirements within SP 800-171 via the provided comment template (the Excel document). Please do not hesitate to contact me if you have any questions. Thank you for the opportunity to contribute to the work of NIST.

Thank you,

Ian Bell
Policy Analyst
The Coalition for Government Procurement
[redacted]

ibell@thecgp.org

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.	
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?	

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
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.	
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?	

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
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 others)	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 others)	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.	
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.	

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
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.	
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.	

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
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."