1 Rev3 & 171A Rev3

Comment (include rationale)*
On behalf of the members of NDIA, we appreciate the opportunity to share comments and feedback regarding the final draft version of Revision 3 of the NIST Special Publication 800-171 titled *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* , and the corresponding revisions to NIST Special Publication 800-171A titled *Assessing Security Requirements for Controlled Unclassified Information* . In response to your request for comments, we would submit the following general comments for your consideration and action, as well as the detailed attached comments on both regulations.
Our members are very appreciative to NIST for the open process that has been utilized to advance these revisions, including briefings, open meetings and conversations with industry and other stakeholders to share details and help to fully understand the changes and what they will mean in practice. We would also like to express our support and appreciation for the concurrent revision, renumbering and release of the assessment documentation found in NIST SP 800-171A. Using a concurrent process aligns the use of the revised standard with the assessment documentation necessary to understand and capture conformance with the standard. Both of these actions are beneficial to the industrial base and government and serve to illuminate the changes and understand as well as possible the changes all can anticipate.
Industry would take this opportunity to call upon NIST to engage and encourage their government partners who utilize these special publications to undertake the necessary additional actions to better safeguard controlled unclassified information as effectively as is possible. In order to achieve that goal, it is imperative that government specify and clearly define controlled unclassified information (CUI), complete the promulgation of associated contracting clause regulations, and, most importantly for the success of this undertaking, impose and implement an effective document marking process for all government agencies to utilize. Without these actions, industry cannot effectively, consistently, and successfully protect CUI and government should not expect their information to receive the level of protection these standards and the corresponding contracting clauses seek to achieve.

Industry would also point to a lack of clarity and delineated approach to phase the adoption of these standards, the corresponding assessment documentation, the current assessments and audits conducted pursuant to Defense Federal Acquisition Regulations Supplements (DFARS), the appearance of new DFARS clauses implementing the Cybersecurity Maturity Model Certification 2.0 (CMMC) in contracts and the corresponding revision of all guidance and training materials related to the assessments and accreditation the Department of Defense seeks with CMMC.
The NIST standards are expected to be finalized in early 2024, including the assessment documentation in 800-171A, but industry continues to invest in a conformance model based on Revision 2 of 171 and Revision 1 of 171A. The FAR and DFARS clauses reliant on these NIST standards specify that compliance is based on the standard in force at the time of award, which means an industry partner or vendor may have to invest in and maintain compliance under Revision 2 for some contracts and Revision 3 for others. Further confusing things, the accreditation body for CMMC has identified that they will need at least a year after the finalization of the standard in order to revise all documentation, retrain and certify assessors and accredit CMMC Third Party Assessment Organizations (C3PAOs). Finally, the CMMC regulations position industry to be reliant upon these misaligned revisions, updates, and effective dates, all of which creates a substantial challenge for industry to understand and implement in an effort to protect CUI.
NDIA would strongly recommend and encourage NIST to work with the FAR and DFARS Councils, the DoD CIO office and the Cyber AB to develop a phased approach to the transition from Revision 2 to Revision 3, with clear implementation dates and milestones indicating when industry should shift investments in cyber protections for data from previous iterations of the 800-171 standards to the latest version. Without clearly delineating effective dates, and having a phased implementation period, the government risks having to maintain, assess and audit multiple, varying standards that employ differing assessment tools and guidance across hundreds of thousands of industrial base partners. This misalignment can and should be addressed prior to the imposition of Revision 3 upon the effort to protect CUI in Nonfederal Systems and Organizations.
Overall, the increased specificity of the controls is improved. Thank you.
The overall organization of 171r3 is better than in r2. Thank you.

In some of the controls, "system" refers to a single computer (sometimes it is referred to as a component, other times not). Sometimes components appear to be part of an individual computer such as the storage device(s). In other cases, the "system" applies to a network of systems, potentially spread across may physical locations and even states or countries. Sometimes "system" seems to include non-computing items such as lockable doors or desk drawers protecting CUI. It would be helpful to clarify this distinction and/or be
Few companies work solely for one government agency. Since each one can define their own ODPs, the result is a substantial workload and hence increase in cost to the government for tracking each agency's ODPs. It would be better if either NIST set the ODPs or NIST collects all of the ODPs from the different agencies so there is one place for us to find them.
Rather than commenting for each one, NDIA noticed that in 800-53, the *-01 controls are all for policy and procedures. Policy and procedures are required to effectively maintain confidentiality. 3.15.1 requires policy and procedures (P&P), so making the audit requirements for P&P explicit ensures that organizations will include
For 171A, how are OPDs to be handled if no customer has defined an OPD value?
800-171 Rev3
Comment (include rationale)*
In the discussion section, please provide examples of specifications. For example, for regular user accounts, presumably Active Directory is not an allowed specification, but the HR database is allowed.
In the discussion section, give examples of allowed and disallowed authoriztions. For example, presumably a properly-approved ticketing system ticket to set authorizations is OK, but a verbal communication without a corresponding log trail is not.
Why did 800-53 AC-02[j] get tailored out? Regular reviews of accounts should be performed to protect CUI confidentiality. Without this being specified, organizations will not do it.
The discussion mentions "pattern hiding displays", but these are no longer mentioned in the control itself. The relevant portion of the control is [c].
Can you be more specific about the "terms, conditions, and security requirements?" It is somewhat covered in the discussion, but making a risk-based approach more clear would help organizations decide which controls on the terms, conditions, and security requirements are appropriate.
Include 800-53r5 AC-22[a]. This will make assessment easier because the requirement for limited people posting publicly is more clear.

Include 800-53r5 AT-01[a][1]. Having the extra specficity for what must be covered will help deal with different ideas for what level of training is required.
Include AU-06(5). Correlation abilities are effecively necessary for organizations beyond a few employees or systems, ad even those small setups can benefit from correlation abilities. Additionaly, 800-171Ar3 lines 1054 and 1055 require correlation.
Define "high risk location".
Per the glossary, a "system" is an "information system". Please elaborate on how system media can be non-digital. I presume you mean, for example, paper, but this is unclear because information systems other than printers do not process paper media. This relates to the general comment that "system" is unclear.
The discussion mentions cryptographic methods, which appear in 800-171Ar3. However, these are never mentioned in the requirements.
Similar to 3.8.2, again, non-digital system media makes no sese. I presume you mean, for example, printed media, but that is not "system media".
The control says that egress must be controlled. How can this occur with physical keys? Exit doors must allow egress in emergency situations such as fire, so doors requiring keys on both sides will violate fire codes. In general, describing the requirements for egress control needs more detail.
Define "visitor". Is a visitor anyone without approved access to a facility?
Presumably "distribution and transmission lines" are for computer networks. Or, are they for power? Or voice phone system? Or all of these? Please clarify.
The risk of unauthorized disclosure to a DIB company is little more than they will lose the ability to get contracts. I think that you want organizations to perform a risk assessment for events that could lead to an unauthorized disclosure of CUI.
The system boundary was required by r2 3.12.04. See comment for 3.15.02, and cosider referencing 3.15.02 if the required boundary is put back. Otherwise, this control contains an implied requirement for a boundary without an explicit control.
What if a known system vulnerability is not directly an issue related to one of the controls in 800-171 and it has a low proaibilty of exploit or high complexity. If Management has declared that it accepts the risk, is this acceptable?
In the discussion, please mention a responsibility matrix as part of satisfying requirement [b]. It is hinted at, but making this requirement more explicit would help. We do see that it is more explicit in 3.16.03b, so a forward reference to that would be sufficient.

The system boundary was required by r2 3.12.04. Now, there is an implied requirement for a boundary without an explicit control specifying that the boundary must exist. Additionally, if an organization is completely and correctly implementing Zero Trust, is a boundary still required?
It would be helpful to add into the discussion the commonly-used terms of "data in motion" and "data at rest". Doing so might help people with less familiarity understand what is required.
In the discussion, please make it more clear that the camera and microphone on a laptop or mobile device such as phone or tablet is part of a collaborative computing device when conferencing software such as Zoom, Teams, etc is in use. Traditionally, organizations have only considered this control as applying to specific conferencing systems such as a Polycom Soundstation.
Since this control applies to laptops etc., it is worth ensuring that users are trained to know the indications of use.
In r2, 3.12.4b explicitly required a system boundary to be defined. This control was incorporated into 3.15.2, but the requirement for a defined boundary disappeared.
This control is vague. As we read it, for example, this says to follow DFARS 7012, Section 889, etc. Can you make it less vague, possibly by including examples of what you mean?
In the discussion, please mention a responsibility matrix as part of satisfying requirement b. In general, how does this control relate to 3.12.05 which seems to cover similar concepts?
Why does this control not reference NIST SP 800-161? Or is "800-160-1" a typo?

0-171A Rev3

Comment (include rationale)*
Nothing says that risks associated with individuals are being watched.
You cannot enforce CUI flow without first documenting the flow. 3.04.11 sort of goes there, but does not cover flow.
CUI spills normally need to be reported to the appropriate government agency. No determination statements cover this.
You cannot verify the records are retained unless a retention period is defined somewhere.
Here is an example, where system appears to refer to a single computer (see row 6 in this spreadsheet). Baselines need to exist for every OS in use, and, for server OSs, the applications that run on them (web, database, file, etc.).

This is nearly impossible for an agency to define as an ODP. The non-federal organization needs to be the one specifying the configuration settings. It is OK to say that they have to be restrictive, but our customers cannot know what is appropriate in our environment. Finally, these configuration settings are a part of the baseline described in 3.04.01.
Similar to 3.04.02, this is effectively impossible for agovernment agency to specify for a contractor.
The control discussion disucsses non-digital media. But none of the determination statements address this.
In most assessment objectives, you broke the control into its parts. But not here. Should this be three? 1. System media that contain CUI are sanitized prior to disposal. 2. System media that contain CUI are sanitized prior to release out of organizational control. 3. System media that contain CUI are sanitized prior to release for reuse.
Why is A.03.10.07.ODP[01] not part of A.03.10.07.c? This is where it is used.