From:	[redacted] via 800-171comments
To:	800-171comments@list.nist.gov
Cc:	[redacted]
Subject:	[800-171 Comments] DOE Comments: Draft NIST SPIM-20 RE: Draft NIST SP 800-171 Revision 3, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
Date:	Friday, July 14, 2023 10:48:18 AM

Good Morning –

Below are comments for consideration on Draft NIST SP 800-171 Revision 3, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Please let us know if we can further assist.

1. p. 4 Lines 79-86, p. iii, change summary, p. 91, Change log, lines 3063-3064:

Comment: The introduction of organization-defined parameters (ODP) in Initial Public Draft of NIST SP 800-171r3 will not be implementable when the requirements in NIST 800-171 are applied in contracts. The document states that the ODPs are to be established by the USG. When a company has more than one contract with the Federal Government, each contract entity will be required to identify the parameters, and will inevitably have differing requirements from agency to agency and even within agencies. This will drive confusion and inefficiencies for contracting officers and the contractors accountable for the security requirements. The intent for NIST SP 800-171 was to identify security requirements in such a way that inherently governmental requirements were removed and there was flexibility to allow the contractor to implement solutions that meet the intent of the requirement without over specification.

Recommendation: Remove the ODPs. Either reword requirements to capture the intent of the requirement without ODP, or define the parameters specifically in the document by including a nominal value or range of values as appropriate. Do not leave this open to all contracting entities to write in their own parameters.

Rationale: NIST SP 800-171 applies to contractors' internal IT systems. Contractors use their systems for all aspects of their business and so use it to provide products for multiple customers, including multiple USG agencies (and often multiple elements within a particular agency).

- Under the proposed construct agencies (or multiple elements within an agency) would specify different parameters, making it extremely difficult for the contractor to manage his system with the parameters constantly changing and/or conflicting.
- Under the proposed construct, agencies might require one set of values for one contract and a different set for another contract – so the contractor would be contractually bound to do different things by the same agency or element within an agency. Not a tenable situation.

- Under this construct, there will be no one set of requirements for contractors to implement.

In addition to the challenges for contractors, this proposed construct will have an adverse impact on the Government (Requiring Activity/Program Office/Contracting Officer).

- If ODPs are required, then for every contract where NIST SP 800-171 is invoked, the Requiring Activity/Program Office will have to populate the ODPs.
- While ODPs are acceptable for USG purposes in NIST SP 800-53, the organization sets the parameters for themselves, consistent with the organization's policies. The contractor does not have that option if every contract with every agency differs. The amount of time spent by the government to identify OPDS in every contract, combined with the time spent by the contractor to track and assess compliance with every different contractually required ODP is prohibitive.

This is a nontrivial problem. The estimated number of individual contractors doing business with the USG that might deal with CUI is about 73K. It's estimated that about 24K of these contractors will have at least one contract award that will involve CUI each year. But many contractors will have many contracts each year that will involve CUI – larger contractors may have a thousand contracts a year, smaller contractors might have 10 or 100 contracts. The number of contracts that actually will have to implement NIST SP 800-171 and have the ODPs filled in is conservatively well over 100K per year.

It is noteworthy that in the NIST SP 800-171r3 FAQs, NIST notes that "Federal agencies can elect to specify ODPs, provide guidance on selecting ODPs for nonfederal agencies, or allow nonfederal agencies to self-select ODP values." However, the Initial Public Draft does NOT imply such flexibility: "For some requirements, organization-defined parameters (ODP) are included. These ODPs provide additional flexibility by allowing federal organizations to specify values for the designated parameters, as needed. Flexibility is achieved using assignment and selection operations. The assignment and selection operations provide the capability to customize the requirements based on organizational protection needs. Determination of organization-defined parameter values can be guided and informed by laws, Executive Orders, directives, regulations, policies, standards, guidance, or mission and business needs. Once specified, the values for the organization-defined parameters become part of the requirement.

- The guidance in 800-171r3 will not be interpreted as 'optional' by Agencies.
- And, if left to interpretation, agencies that elect to specify ODPs will surely be in conflict with each other and the values implemented by the nonfederal organization.

2. **Recommendation:** Reconsider the requirements for policy and procedures (AC-1, AT-1, AU-1 CA-1, CM-1. IA-1, IR-1, CP-1 MA-1, MP-1).

Rationale: In previous versions, policies were expected to be routinely satisfied without specification by the federal government. Introducing this as a specific requirement will

inevitably increase costs. Requiring Activity/Program Office/Contracting Officers may require specific formats for ease in assessing the implementation of the requirements. If every agency/ Requiring Activity/Program Office/Contracting Officer has a different requirement for how the policy should be constructed and conveyed, this will increase confusion and cost to the government.

3. **General Comment:** The recasting of the security requirements into NIST SP 800-53 type requirements/controls increases the specificity of the requirements and reduces flexibility for non-Federal entities. The intent for NIST SP 800-171 was to enable non-Federal entities to secure sensitive information at the moderate baseline without driving specific solutions that will increase cost or in some cases be unattainable. The long-term impact is to reduce the number of eligible contractors who can meet the security requirements, increasing costs to the government, and driving away small and disadvantaged businesses.