From:	800-171comments@list.nist.gov on behalf of [redacted]
To:	800-171comments@list.nist.gov
Subject:	[800-171 Comments] Boeing - NIST 800-171r3 IPD Comments & Cover Letter
Date:	Friday, July 14, 2023 4:21:27 PM
Attachments:	NIST_800-171r3_Boeing_Cover_Letter_FINAL_14Jul2023.pdf sp800-171r3-ipd_Comments_Boeing_14Jul2023.xlsx

---

Dr. Ross & Ms. Pillitteri,

Thank you for the opportunity to submit Comments on the recently released NIST 800-171r3 IPD. Boeing looks forward to collaborating with you and our industry peers to ensure that we enable the industry as a whole to raise their cybersecurity posture to protect CUI and other sensitive data types.

On behalf of Boeing,

Joe Degnan
Boeing Enterprise Security
[redacted]

The secret of change is to focus all of your energy, *not on fighting the old*, but on *building the new*.
Socrates

The Boeing Company
929 Long Bridge Drive
Arlington, VA 22202

July 14, 2023

Dr. Ron Ross & Ms. Victoria Pillitteri
National Institute of Standards and Technology
Computer Security Division, Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Re: NIST Special Publication 800-171, Revision 3

Dear Dr. Ross and Ms. Pillitteri:

I write on behalf of The Boeing Company ("Boeing") to share comments and feedback on the initial public draft of NIST Special Publication 800-171, Revision 3, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, published on May 10, 2023. Enclosed please find the comment spreadsheet containing consolidated recommendations from stakeholders across the company.

Boeing's feedback is primarily focused on Organization-Defined Parameters ("ODPs") and its significant impact on industry. Although it is intended to provide flexibility for federal agencies by increasing control over protected data types, the benefits of ODPs are far outweighed by the burden it imposes on contractors and supply chains. Among other things, the implemention of ODPs will create a regulatory landscape that varies per agency, increases costs, slows production, and burdens contractors, particularly small- to medium-size suppliers.

The enclosed comment spreadsheet also includes feedback relating to other proposed changes to the initial public draft of NIST SP 800-171, Revision 3, including re-categorized controls relating to multifactor authentication and Virtual Private Network ("VPN") split tunneling.

Given the revised draft's likely impact on industry and existing compliance regimes, Boeing would encourage NIST to continue engaging the private sector, including industry assocations, and consider additional points of view as it works to further revise NIST SP 800-171, Revision 3.

Boeing appreciates the opportunity to comment on the initial public draft of NIST SP 800-171, Revision 3 and would welcome an opportunity to discuss our recommendations directly. Please do not hesitate to reach out to me directly at [redacted] if there is any additional information we can provide.

Best regards,

Howard L. Alexander
Director, Governance, Risk & Compliance
Boeing Enterprise Security

Attachment: sp800-171r3-ipd_comments_Boeing (.xlsx)

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Boeing	General	Publication	0	N/A	Additional clarity and transparency with closer collaboration with NIST USG and private sector experts.	As a result of the broad use and popularity of the NIST series of standards by Federal Agencies and other domestic and foreign entities in contractual obligations it is recommended that NIST share some background on the drafting and updates to standards and formalize the adjudication of comments. It is also recommended that NIST work with subject matter experts from both industry and government to discuss and reach consensus on changes to its standards which are of increasing importance and directly impact many thousands of non-federal organizations in the U.S. and around the world.
2	Boeing	General	Publication	2	N/A	Due to the nature of enterprise and now cloud computing NFO information systems have been built based on specific technologies that are not common across industry. These systems have been tuned to a company's risk tolerance and any changes mandated by a many different federal agencies or departments would cause significant changes to NFO architecture and practices (cloud SaaS IaaS PaaS etc.) that are being used to support federal agencies missions and purpose. NFO information systems are also used to support other entities including commercial entities via appropriate segregation that are subjected to other regualtions and requirements beyond 800-171 and in some instances could conflict with 800-171 ODP's defined by federal agencies. It also negates and significantly complicates assessments due to the variability of ODP's from a variety of non-coordinated stakeholders. As such each contract could require the re-write of process policy and procedures within a information system that conflicts with another contract by a separate federal agency.	Allow non-federal organizations (NFOs) the ability to identify ODP's within their own information system(s) and let NFOs define and explain how their information system protects CUI data via System Security Plans interviews with non-federal organization SMEs or attestation. The significant variabilty introduced by enabling federal agencies to outline ODP's without the benefit of knowing how a contractor's enterprise network is configured is problematic. When applied to companies with numerous federal contracts the change in requirements would be signifcantly burdensome resulting in varying and inconsistent compliance and raising costs. The current DCMA DIBCAC Assessment methdology allows for proper Basic Medium and High assurance assessments of non-federal organizations and should be used as a model/guide for future assessments where NFOs can define ODPs and then demonstrate compliance by attesting or providing evidence.
3	Boeing	General	Publication	3	64	This section as written seems to enable Federal Agencies contracting with the non-federal organizations to implement security controls relating to each requirement based on their unique information system technology and enterprise architecture.	While ODPs may remain the shift should occur whereby the ODP is defined by the non-federal organizations vs. the federal agencies. Due to the potential for extreme variations related to those ODPs without the benefit or knowledge of how a non-federal organizations network is configured and what technology is being used to support the protection of CUI intellectual property information of others etc. it could cause major disruptions and conflicts between federal agencies.
4	Boeing	General	Publication	4	79	The flexibility of ODPs intended for federal agencies would significantly complicate compliance and is burdensome. The proposed ODP framework does not take into account controls that non-federal organizations already have in place to protect CUI. It does not consider how ODPs across all federal programs departments and agencies could be too numerous for federal contractors to comply with and adequately protect CUI.	The variability of ODP requirements across all contracts could be too numerous for a federal contractor to comply with. The "flexibility" across "executive departments" possible through ODPs increases the burden for all NFOs who would have to comply with countless and likely conflicting/differing ODP's issued by executive departments and agencies. This variability would have a cascading effect on not only on prime contractors but also their multi-layered supply chain which would also be subjected to the same ODP requirements. We recommend that NIST convene experts from government and industry including Sector Coordinating Councils and Government Coordinating Councils to create a consistent baseline of ODP's for use across all the executive departments that can be changed at clearly-defined intervals with consultation from NFOs.
5	Boeing	Technical	Publication	27	1025	3.5.3 specifies a blanket requirement for MFA to all system accounts which is technically impossible to implement in a number of conditions including but not limited to: 1. OS-local administration accounts such as Windows "Administrator" or Linux Root". 2. Application-specific service accounts. 3. All user accounts on standalone (non-networked) systems.	Permit NFOs to specify the conditions under which single factor authentication is permitted.
6	Boeing	General	Publication	46	1716	This requiremenet does not clarify whether an assessment can be performed by internal or external providers and it does not describe the frequency of these assessments.	Clarify this control with regards to whom is allowed to perform the assessment and provid more clarity to contractors on what type(s) of assessment will require independent assessment; whether the ability to provide attestations/assessments by internal groups for an organization is allowed; and what can be done if a company doesn't have the resources to complete an independent assessment.
7	Boeing	Technical	Publication	49	1845	3.13.7 Split Tunneling (reference to ODP): ODP is specific to implementation and seemingly do not provide value as long as there is compliance with the control. ODPs define the safeguards - What f one customer says use a VPN and another says do not use a VPN? The ODP variability is difficult to standardize if multiple customers enforce different parameters.	Rather than letting each department or agency create separate ODPs NIST may consider publishing ODP baselines that could be used for contracts with modifications only being required on specific instances where additional security or other tailored contols are needed. NIST or federal authority (NARA OMB) should publish a baseline range and/or guidance for the ODPs that could/should be used for the majority of contracts with modifications only being required on specific instances where additional security is needed but then should/could be additional requirements rather than changing the baseline. For example for encryption/cryptography publish guidelines for identifying strong crypto/encryption and not just pointing to the NIST 140-X series but rather the steps to prove strong encryption/crypto. Another example would be the timeline ODPs would be defined as Annually at a minimum.
8	Boeing	Technical	Publication	60	2300	What if one agency demands the use of its standard solution and that contradicts the choice of another agency?	The intent of ODP's is laudable but deferring to individual departments and agencies is problematic and will generate a varied compliance framework that will be difficult to comply with and costly.
10							
11							