From: [redacted] via 800-171comments
To: 800-171comments@list.nist.gov
Cc: [redacted]
Subject: [800-171 Comments] RTX comments submission for NIST SP 800-172 Rev. 3 (Initial Public Draft)
Date: Friday, January 17, 2025 12:00:00 PM
Attachments: NIST 800-172r3 IPD - RTX Comments - FINAL - 17Jan25.xlsx

---

Please see attached comments list from RTX for the NIST SP 800-172 Rev. 3 (Initial Public Draft), Enhanced Security Requirements for Protecting Controlled Unclassified Information.

Thank you for soliciting and considering our comments.

Best Regards,
Angie Bull

Angela Bull, CISSP
Cybersecurity Compliance
[redacted]
RTX

NIST SP 800-172r3 ipd - Initial Public Draft

Comment Number	Submitted By (Name/Org):	Type (General/Editorial/ Technical)	Starting Page #	Starting Line #	Comment (include rationale)	Suggested Change
1	RTX	General	6	338	We remain concerned with agencies having the option to set differing Organization-Defined Parameters (ODPs). The stated objective of Executive Order (EO) 13556 is to establish a governmentwide program to standardize the handling of Controlled Unclassified Information (CUI). Allowing federal agencies to use ODPs to define unique requirements is contrary to the objective, as it promotes inconsistent and potentially competing standards across the federal government. Agency baseline expectations will diverge resulting in a patchwork approach to cybersecurity, rather than allowing a single baseline standard as intended. Companies supporting multiple agencies and contracts will incur significant cost implicattions to meet the unique controls across multiple agencies and contracts, and may determine that some requirements are too costly to implement based on financial/risk analysis. Having these contradictory ODP requirements across agencies will make it difficult for companies to fully comply and will create operational challenges and significant cost implications to meet unique controls by agency or contract. Moreover, while government contracting offices are competent with procurement rules and able to determine when certain requirements can be waived, they may not be able to define detailed ODP requirements or cybersecurity-related controls. There is also no known cadence for managing changes to ODPs, so agencies could change ODPs at any time (unlike revisions to SP 800-172 which are published with a formal comment period). Lastly, SP 800-172 is becoming more recognized and accepted globally. Allowing varying ODPs across federal agencies will weaken the NIST “standard” making it less effective and less likely to achieve reciprocity with other standards.	We recommend NIST work with government and private industry to establish standard ODP values that can be implemented uniformly.
2	RTX	Technical	14	561	**03.01.10e—Object Security Attributes.** This requirement requires segregating data into certain enclaves based on the security attributes associated with that data. For example, data labeled "XYZ" could only flow to destinations labeled "XYZ" and no other areas. This requirement can force companies to implement several enclave solutions depending on how the Object Security Attributes are organizationally defined (e.g., "XYZ", "ABC"). This will result in significant cost and feasibility implications to meet unique controls by agency or contract.	We recommend withdrawal or NIST work with government and private industry to establish standard ODP values that can be implemented uniformly.
3	RTX	General	33	1175	**03.09.04E—Citizenship Requirements**. This requirement requires organizations to "verify that individuals accessing a system processing, storing, or transmitting CUI are U.S. citizens." Given some types of CUI may be accessed by non-U.S. citizens, it is unclear if NIST intends, as written, that access to systems storing, processing, or transmitting any CUI, irrespective of whether such CUI is itself restricted to U.S. citizens (e.g., no foreign dissemination or NOFORN), must be limited to U.S. citizens, or if NIST erred and intends that such verification must only occur where the type of CUI is appropriately restricted to U.S. citizens (i.e., by the underlying law, regulation, government-wide policy, or limited dissemination control).	If NIST intends the former, it may represent an unnecessary restriction on access to CUI and run counter to the goals of the CUI program, and we recommend NIST withdraw the control. If NIST intends the latter, we recommend NIST qualify that the control only applies where the CUI itself is restricted to U.S. citizens (e.g., "Where required, verify that individuals accessing a system processing, storing, or transmitting CUI are U.S. citizens.").
4	RTX	Technical	47	1621	**03.13.04E—Isolation of System Components.** For non-federal organizations who contract with multiple federal organizations, this requirement could require implementing enclave solutions to meet individual federal organizational requirements. This additional complexity to a company's network architecture, resulting from enclave solutions, will result in significant cost and feasibility implications to meet unique controls by agency or contract.	We recommend removal of cross-domain device requirements as those are intended for higher security boundaries (e.g., classified), not lower security boundaries (e.g., unclassified). Alternatively, we recommend NIST work with government and private industry to establish standard ODP values that can be uniformly implemented by non-federal organizations.
5	RTX	Technical	50	1722	**03.13.09E—Security Tool, Mechanism, and Support Component Isolation**. The primary concern with this requirement is the explicit indication of utilizing physically separate subnetworks (at Layer 3), which does not allow for using logically separate subnets (at Layer 2). This requirement could require an overhaul of the network architecture for established organizations that utilize logically separate subnets, resulting in significant time and cost or forcing an organization into an enclave solution.	We recommend adding in the option for utilizing physically or logically separate subnets.