From:	800-171comments@list.nist.gov on behalf of NDISAC Info
To:	800-171comments@list.nist.gov
Subject:	[800-171 Comments] ND-ISAC COMMENTS RE NIST 800-171 R3 FPD
Date:	Friday, January 26, 2024 4:33:15 PM
Attachments:	ND-ISAC_Comment_NIST 800-171 R3 FPD_26JAN2024.pdf

ALCON

Please see comments attached representing the views of the National Defense Information & Analysis Center member companies. Thank you for the opportunity to comment.

V/r
Info@NDISAC.org

_____

Submit Your Comments

The public comment period is open now through ~~January 12~~ January 26, 2024. We strongly encourage you to use this comment template if possible, and submit it to 800-171comments@list.nist.gov.

Reviewers are encouraged to comment on all or parts of draft NIST SP 800-171, Revision 3. NIST is specifically interested in comments, feedback, and recommendations for the following topics:

- Re-categorized controls (e.g., controls formerly categorized as NFO)
- New tailoring criterion (e.g., other related controls [ORC])
- Inclusion of organization-defined parameters (ODP)
- New or revised requirements
- Prototype CUI overlay

Comments received in response to this request will be posted on the Protecting CUI project site after the due date. Submitters' names and affiliations (when provided) will be included, while contact information will be removed.

Please direct questions and comments to 800-171comments@list.nist.gov.

National Defense Information Security and Analysis Center
1050 Connecticut Ave NW #500, Washington, DC 20036
www.ndisac.org | (202) 888-2724 | info@ndisac.org

January 26, 2024

Dear Dr. Ross and Ms. Pillitteri

Reference: Invited comments -- Ross R, Pillitteri V (2023) ***Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations***. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-171r3 fpd

Thank you for the opportunity to provide feedback on the NIST SP 800-171, ***Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations Final Public Draft***, dated November 2023. ND-ISAC member companies respect and regard NIST's role as indispensable in developing recommendations and guidance for science-based cybersecurity technical controls. Based on extensive review, ND-ISAC cybersecurity subject matter experts within our technical working groups respectfully encourage the following overarching perspectives:

- NIST should consider performing a series of table-top exercises combining subject matter experts from government and industry to identify impediments &/or the most effective approaches in using publications and implementation resources to apply the CUI Requirements Overlay before IOC. This would permit NIST to appropriately modify guidance with the desirable effect of accelerating IOC objectives, but also better align the guidance with companion cybersecurity publications NIST 800-53, 800-53B, and 800-53A. To enable this NIST should delay the release of Revision 3 Final Public Draft.

- NIST should partner with key Industry stakeholders to collaborate on developing flexible and risk-based selections for systems development across an operational life cycle based on the Risk Management Framework (RMF) and Cyber Security Framework (CSF). This approach would enable the development of a recommended menu of relevant and effective Organization Defined Parameters (ODPs) responsive to the great majority of probable use cases. This approach would create considerable efficiencies for federal agencies in applying ODPs, with corresponding benefits to industry in effectively managing ODPs and forecasting cost impacts.

- NIST should consider an “agile” approach in the development and delivery of new or updated standards similar to the iterative delivery of software improvements. This approach augmented with tools to facilitate industry input, tracking, and metrics; would greatly benefit adoption of standards by communities affected by NIST standards. This would enable ongoing incremental adoption in preference to expansive short-fused changes in security controls. An iterative approach would moderate operational impacts of NIST guidance changes to federal agency cybersecurity policy and regulations, and associated requirements to implement security controls.

The ~150 member companies of ND-ISAC are committed to contributing to the improved cybersecurity and resilience of the Defense Industrial Base. In that spirit, we look forward to collaborating with NIST to develop fruitful and effective approaches to achieve that. Thank you again for the opportunity to submit these comments.

V/r

STEVEN D. SHIRLEY
Executive Director