ANDREW N. MAUER
Senior Director
Regulatory Affairs

1201 F Street, NW, Suite 1100
Washington, DC 20004
P: 202.739.8018
anm@nei.org
nei.org

NUCLEAR ENERGY INSTITUTE

April 1, 2022

Mr. Scott Flanders
Deputy Chief Information Officer
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: NRC's Controlled Unclassified Information Program Implementation

Project Number: 689

Dear Mr. Flanders:

The Nuclear Energy Institute (NEI)[1], on behalf of our members, is writing to express our concerns that the Nuclear Regulatory Commission (NRC) staff's proposed approach for NRC Controlled Unclassified Information (CUI) rule implementation is unduly burdensome and unnecessary and NEI recommends that an alternate approach be pursued. The expectation for stakeholders to implement an information system consistent with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," is not justified for external stakeholders that do not wish to receive and download CUI electronically from the NRC. This appears to be in direct contradiction with the NRC's CUI Statement of Policy which states that NRC is committed to avoiding unintended consequences that unnecessarily increase burden on external stakeholders.[2] While NEI recognizes that in order to receive and download CUI electronically the NIST standards are expected to be followed, receiving CUI electronically is only one means of receiving information and the decision to establish a suitable system will be made by each company. It should not be unilaterally imposed as a prerequisite of receiving CUI from the NRC.

NEI's members are fully committed to maintaining the protocols that are in place today for safeguarding Sensitive Unclassified Non-Safeguards Information (SUNSI) as the NRC transitions to CUI. We understand that the CUI program is intended to standardize the way the executive branch handles unclassified information that is sensitive and merits special controls to prevent unauthorized access. Our members

[1] The Nuclear Energy Institute (NEI) is responsible for establishing unified policy on behalf of its members relating to matters affecting the nuclear energy industry, including the regulatory aspects of generic operational and technical issues. NEI's members include entities licensed to operate commercial nuclear power plants in the United States, nuclear plant designers, major architect and engineering firms, fuel cycle facilities, nuclear materials licensees, and other organizations involved in the nuclear energy industry.
[2] The Statement of Policy states, "The NRC is committed to avoiding unintended consequences that unnecessarily increase the burden on external stakeholders while also maintaining adequate protective measures for CUI." (Docket ID NRC-2021-0204)

appreciate the need to protect CUI from unauthorized access and we remain duly committed to working with the federal government to ensure its protection. Our members' interests lie in guaranteeing the proper protection for the information in the most effective manner.

While we recognize that following the NIST standard is a National Archives and Records Administration (NARA) requirement, NRC's compelling its stakeholders to implement a NIST SP 800-171 information system standard would be an impediment to information sharing which is in direct contradiction to the purpose of the initiating Executive Order based on the Presidential Task Force Report[3] (the Report) that prompted the executive order. While the NRC has indicated that industry organizations must implement a NIST information system standard, the Report foresaw the challenges with mandating federal IT standards,[4] and stated that raising the level of information system safeguards was not among the factors driving the need for the establishing the CUI framework.[5] Furthermore, regarding non-federal agencies, the Report states that "these entities are neither required by law to comply with the same physical or IT safeguarding standards as the federal Executive Branch, nor are they necessarily funded to do so," and continues to say later that guidelines and safeguarding standards should be "achieved with reasonable and appropriate efforts by the nonfederal partners."[6] The burdensome nature of compliance to the NIST SP 800-171 standard represents neither reasonableness nor appropriateness, and forcing stakeholders to comply could actually impede the sharing of information where resources constraints on non-federal agencies may compel them not to comply.

Our understanding is that the NRC is aware of the challenges that adoption of the NIST standard places on its stakeholders and is actively pursuing alternative methods to ensure that CUI can continue to be efficiently and effectively shared with stakeholders. The NRC already has successfully established methods of making SUNSI information available on electronic portals, including the protected web server for sensitive security information. We urge the NRC to adopt a primary approach to share CUI with its stakeholders that is based upon access to CUI through electronic portals, with hard copies of documents also provided through the U.S. mail. This approach will minimize burden on NRC's stakeholders and allow continued reliance on NRC's well-established requirements and guidance for the safeguarding of SUNSI, which is appropriate for CUI and consistent with the CUI rule. Should any NRC stakeholders wish to receive CUI electronically from the NRC, they can elect to adopt the NIST standard.

We appreciated the opportunity to share our concerns with the NRC during the March 28, 2022, public meeting and to review the draft nondisclosure agreement (NDA), which we are evaluating for further comments. That meeting was the first time the NRC communicated the implementation date of September 20, 2022. Given that several unanswered questions remain about the timeline and actions needed to

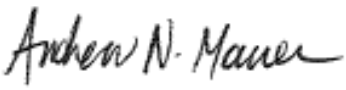
[3] "Report and Recommendations of the Presidential Task Force on Controlled Unclassified Information," dated August 25, 2009 (the Report)
[4] Section 3 of the Report states, "The Task Force is concerned, however, that incorporating existing federal IT standards directly into the CUI Framework could pose a significant impediment to CUI implementation . . . ."
[5] Section 10 of the Report states, "Raising the level of IT safeguards, however, was not among the factors mandating the replacement of the existing 107 disparate SBU regimes, the development of the CUI Framework, or the expansion of the CUI Framework beyond its current scope."
[6] See "Report and Recommendations of the Presidential Task Force on Controlled Unclassified Information," (pages 17-18)

support that implementation date, our view is that requiring external stakeholders to commit time and resources toward the implementation of a NIST SP 800-171 information system standard while the NRC concurrently explores an alternative method is not consistent with the Principles of Good Regulation. It is unreasonable to expect stakeholders to commit time and resources before understanding all of the options that exist to ensure adequate protection of CUI. We request that the NRC explore alternative methods of sharing CUI and delay the implementation of the CUI program until such time that alternate methods can be made available.

In summary, imposing the NIST SP 800-171 information system standard on stakeholders in the absence of alternative methods is unduly burdensome and unnecessary. We appreciate the NRC's consideration of the approaches described in this letter and stand ready to work with the NRC to develop a more practical path forward.

If you have questions on this matter, please contact me or Melody Rodriguez at 202-739-8086.

Sincerely,



Andrew N. Mauer

Enclosure (mailing) or Attachment (e-mail)

c: Michael King, NRR/NRC
Craig Erlanger, NSIR/NRC
Robert Lewis, NMSS/NRC
Tonya Mensah, OCIO/NRC