

From: [REDACTED] [via 800-171comments](#)
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] NIST 800-171 R3 Comments
Date: Wednesday, June 21, 2023 12:42:04 PM
Attachments: [image001.png](#)
[Copy of NIST 800-171- Nuclear CUI- DC Comments.xlsx](#)

The biggest concern from an entity is trying to control CUI on portable media which is on the corporate network. Controlling portable media on the nuclear network is easier as it has already been established and is part of the NCR regulations. Portable media on the corporate network is not cost effective and trying to track who has what portable media is not feasible. If an entity issues out portable media to employees, what happens if the portable media is lost, stolen, or if the employee quits, dies or retires. An entity is limited on the recovery of the portable media and who knows what information is being stored on the portable media.

If CUI is treated as safeguards information or has the same stipulations as safeguards information, it will be more feasible for an entity to control access, and portable media. Also there cannot be any remote access into a system with SGI, so that issue will also be solved.

Tosh Keele, MS | Analyst, Sr Lead
CSO-Security Regulations
Entergy - Office of the Chief Security Officer (CSO)



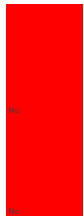
“The secret is to work less as individuals and more as a team. As a coach, I play not my eleven best, but my best eleven.” ~ Knute Rockne

This message is intended for the exclusive use of the intended addressee. If you have received this message in error or are not the intended addressee or his or her authorized agent, please notify me immediately by e-mail, discard any paper copies and delete all electronic files of this message.

System and Common controls P. Object on	3.13.11
System and Common controls P. Object on	3.13.12

Employ FIPS-val dated c yptog aphy when used to p otect the conf dent aty of CUI.

P h b t remote act vat on of collabor at ve comput ng dev ces and p ovide rd cat on of dev ces n use to use s p eant at the dev ce.



FIPS-val dated c yptog aphy s not used

Collabo at ve comput ng s allowed to remote access to p ovide ma ntance support n/o systems w thout a use to be phys ca ly p eant at the dev ce.

Cryptography can be emp oye o support a variety of secu ty solutions including for example the protection of classif ed and Control ed Unc assif ed information the provision of dg tal signatu es and the enforcement of information separation when authorized indiv duas hve the necessary clearances for such information but ack the necessary formal access approvas. Cryptog aphy can also be used to support random number generation and hash generation. Generally app icable cryptographic standards include FIPS-val dated cryptography and NSA approved cryptography. This control does not impose any requirements on organizations to use cryptography. However f cryptography is required based on the se ct on of other secu ty controls organizations define each type of cryptograph c use and the type of cryptography required (e.g. protection of classif ed informat on NSA-approved cryptography prov sion of dg tal s gnatures FIPS-val dated cryptography).

NIST 800-53 B4 defines this control as follows: Control The informat on system
a. Prohib ts remote actvat on of collaborative computing devices with the fo llowing except ons (Assignment organization-defined except ons where remote actvat on s to be a lowed) and
b. Provides an expl c it indication of use to users physically present at the devices.

Supplemental
Collaborative computing dev ces include for example networked white boards cameras and microphones. Ex p c t indication of use includes for example signa s to users when collaborative computing devices are activated.