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 in not feasible. If an entity issues out portable media to employees, what happens if the portable media is lost, stollen, 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)
[redacted]

"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

NIST 800-171 Group ng	N ST 800-171 Requ rement	N ST 800-171 Question	BU/Stake Holders	Does Entergy Meet the NIST 800 171 Requirement (Yes, No, NA)	Does Ente gy Meet the requ ement w th an a ternate measure	NOTES/Alternate Measure	Supplemental Information
Access Cont ol	3.1.19	Enc ypt CUI on mob le dev ces and mob le comput ng platfo ms. ****In Rev 3 moved to 3.1.18***				Ente gy laptops have fu l d sk enc ypt on. Cell phones wh ch can have an Ente gy Ema l account a e not enc ypted. Ce l phones a e managed by a Mob le Dev ce Management Pol cy.	Decisions regarding the emp oyment of mobile code w thin organizat onal information systems are based on the potential for the code to cause damage to the systems f used ma ic ously. Mobi e code technologies include for example Java JavaScript ActiveX Postscript PDF Shockwave movies F ash animations and VBScript. Usage restrictions and implemen ation guidance apply to both the select on and use of mobile code installed on servers and mobi e code downloaded and executed on indiv dual workstat ons and devices (e.g. smart phones). Mob le code pol cy and procedures address preventing the deve opment acqu sit on or introduct on of unacceptab e mob le code within organizational information systems. Related controls AU-2 AU-12 CM-2 CM-6 SI-3.
Access Cont ol	3.1.21	L m t use of po table sto age dev ces on exte nal systems.		No		Ente gy does not cu ently est ct the use of of USB dev ces on the co po ate netwo k. f a USB s connected to a co po ate laptop, the USB w ll be enc ypted and cont o led w th a passwo d befo e the USB can be used.	Lim ts on the use of organization-contro led portab e storage devices in external information systems include for example complete prohibition of the use of such devices or estr ct ons on how the devices may be used and under what cond tions the devices may be used.
Access Cont ol	3.1.22	Cont ol CUI posted o p ocessed on publ cly access ble systems.		No		Ente gy w ll ma k and cont ol all CUI n acco dance w th pol c es , p ocedu es and fede al laws.	In accordance w th federal aws Executive Orders directives pol cies regulations standards and/or guidance the general public is not author zed access to nonpublic informat on (e.g. information protected under the Privacy Act and proprietary informat on). Th s control addresses informat on systems that are control ed by the organization and accessib e to the general pub ic typically without identif cat on or authentication. The posting of informat on on non organization information systems is covered by organ zational pol cy.
Ident f cat on and Authent cat on	3.5.11	Obscu e feedback of authent cat on nfo mat on.		Yes		Ente gy does not have n place mechan sms wh ch would p event obscu e feedback.	The feedback from information systems does not provide information that would allow unauthorized indiv duals to compromise authent cat on mechanisms. For some types of information systems or system components for examp e desktops/notebooks with relatively large mon tors the threat (often referred to as shoulder surfing) may be s gnif cant. For other types of systems or components for examp e mobile dev ces with 2-4 inch screens this threat may be less signif cant and may need to be ba anced against the increased ikelihood of typographic input errors due to the small keyboards. Therefore the means for obscuring the authent cator feedback is selected accordingly. Obscuring the feedback of authent cat on informat on includes for example displaying aster sks when users type passwords into input devices or displaying feedback for a very limited time before fully obscuring it.
Ma ntenance	3.7.3	Ensu e equ pment emoved fo off-s te ma ntenance s san t zed of any CUI. **** n Rev 3, moved to 3.8.3 *****		No		No p ocedu e n place that equ es CUI to be emoved o san t zed f om dev ces befo e the dev ce has been emoved f om nvento y.	This control addresses the information security aspects of the information system maintenance program and appl es to all types of maintenance to any system component (including appl cat ons) conducted by any local or nonlocal entity (e.g. in-contract warranty in house software maintenance agreement). System maintenance also includes those components not directly associated w th information p ocessing and/or data/information retention such as scanners copiers and printers. Information necessary for creating effective maintenance reco ds includes for example (i) date and time of maintenance (i) name of individuals or group performing the maintenance (ii) name of escort if necessary (iv) a description of the maintenance performed and (v) information sys em components/equipment removed or replaced (including identification numbers if appl cable). The level of detail included in maintenance records can be informed by the security categories of organizational information systems. O gan zations consider supply chain issues assoc ated with rep acement components for information systems.
Med a P otect on	3.8.1	P otect (e., phys cally cont ol and secu ely sto e) system med a conta n ng CUI, both pape and d g tal.		No		No cu ent method o p ocedu e to p otect CUI d g tally. The e a e gene al data p otect on pol c es and p ocedu es fo cont oll ng SGI. Phys cal secu ty w ll cont ol and handle pape CUI fo each s te.	Information system media includes both digital and non-dig tal media. Dig tal media includes for example diskettes magnetic tapes external/removab e hard disk drives flash drives compact d sks and d gital video disks. Non-digital med a includes for examp e paper and microfilm. Physically cont olling information system med a includes for examp e conducting inventor es ensuring procedures are in place o a low individua s to check out and return med a to the media library and maintaining accountabi ity for all stored med a. Secure storage includes for example a locked drawer desk or cabinet or a control ed media library. The type of media storage s commensurate w th the security category and/or classif cat on of the information residing on the med a. Controlled areas are areas for wh ch organizat ons provide sufficient physical and procedural safeguards to meet the requirements establ shed for protecting informat on and/or information systems. For med a containing information determined by organizat ons to be in the pub ic domain to be publ cly releasable or to have im ted or no adverse impact on organ zations or individuals if accessed by other than authorized personnel fewer safeguards may be needed. In these s tuat ons physical access cont ols provide adequate protection.
Med a P otect on	3.8.2	L m t access to CUI on system med a to autho zed use s.		No		No cu ent method o p ocedu e to p otect CUI d g tally. The e a e gene al data p otect on pol c es and p ocedu es fo cont oll ng SGI.	Information system media includes both digital and non-dig tal media. Dig tal media includes for example diskettes magnetic tapes external/removab e hard disk drives flash drives compact d sks and d gital video disks. Non-digital med a includes for examp e paper and microfilm. Physically cont olling information system med a includes for examp e conducting inventor es ensuring procedures are in place o a low individua s to check out and return med a to the media library and maintaining accountabi ity for all stored med a. Secure storage includes for example a locked drawer desk or cabinet or a control ed media library. The type of media storage s commensurate w th the security category and/or classif cat on of the information residing on the med a. Controlled areas are areas for wh ch organizat ons provide sufficient physical and procedural safeguards to meet the requirements establ shed for protecting informat on and/or information systems. For med a containing information determined by organizat ons to be in the pub ic domain to be publ cly releasable or to have im ted or no adverse impact on organ zations or individuals if accessed by other than authorized personnel fewer safeguards may be needed. In these s tuat ons physical access cont ols provide adequate protection.
Med a P otect on	3.8.3	San t ze o dest oy system med a conta n ng CUI befo e d sposal o elease fo euse.		No		No cu ent method o p ocedu e to p otect CUI d g tally. The e a e gene al data p otect on pol c es and p ocedu es fo cont oll ng SGI.	This control applies o a l information system media both dig tal and non-digital sub ect to disposal or reuse whether or not the media is considered removable. Examples include media found in scanners copiers printers notebook computers workstations network components and mobile dev ces. The sanitization process removes information from the media such that the informat on cannot be retr eved or reconstructed. Sanit zation techn ques including c ea ing purging cryptographic erase and destruct on prevent the disclosure of informat on to unauthorized individuals when such media is reused or re eased for disposal. Organizations dete mine the appropriate san tization methods recognizing that destruction is sometimes necessary when other methods cannot be app ied to media equiring sani ization. Organizat ons use discret on on the emp oyment of approved san tization techniques and procedures for media containing information deemed to be in the publ c domain or pub icly releasable or deemed to have no adverse impact on organ zat ons or individua s f released for reuse or disposal. Sanit zation of non dig tal media includes for example removing a classif ed appendix from an otherwise unclassified document or redacting selected sect ons or words from a document by obscuring the redacted sect ons/words in a manner equiva ent in effectiveness to removing them from the document. NSA standards and po ic es control the sanit za ion process for media containing classif ed information.
Med a P otect on	3.8.4	Ma k med a w th necessa y CUI ma k ngs and d st but on l m tat ons.		No		No cu ent method o p ocedu e to ma k CUI and l m t d st but on. The e a e gene al data p otect on pol c es and p ocedu es fo cont o l ng SGI.	The erm secur ty marking refers to the appl cat on/use of human-readable secur ty attributes. The term secur ty abeling refers to the app ication/use of security attributes with egard to in emal data structures within information sys ems (see AC-16). Informat on system med a includes both dig tal and non-d gital med a. D gital med a includes for examp e diskettes magnetic tapes external/removable hard disk drives flash drives compact disks and digital v deo d sks. Non-d gital media includes for example paper and microfilm. Security marking is genera ly not required for media containing information determined by organizations to be in the publ c domain or to be publ cly releasable. However some organizat ons may require markings for public information indicating that the information is publ cly releasable. Marking of informat on system med a reflects appl cable federal laws Executive Orders directives policies regu ations standards and gu dance.
Med a P otect on	3.8.5	Cont ol access to med a conta n ng CUI and ma nta n accountab l ty fo med a du ng t anspo t outs de of cont olled a eas.		No		No cu ent method o p ocedu e to cont ol access to med a conta n ng CUI. The e a e gene al data p otect on pol c es and p ocedu es fo cont o l ng SGI.	Information system media includes both digital and non-dig tal media. Dig tal media includes for example diskettes magnetic tapes external/removab e hard disk drives flash drives compact d sks and d gital video disks. Non-digital med a includes for examp e paper and microfilm. This control a so applies to mobi e devices with informat on sto age capability (e.g. smart phones tablets E-readers) that are transported outside of controlled areas. Contro led areas are areas or spaces for which organ zations prov de suff cient physical and/or procedural safeguards to meet the requirements established for protecting information and/or information sys ems. Physical and techn cal safeguards for media are commensurate with the security category or classification of the info mat on res ding on the med a. Safeguards to protect media during transport include for example ocked containers and cryptog aphy. Cryp ographic mechan sms can provide conf dentia ity and integr ty protections depending upon the mechanisms used. Activit es associa ed w th transport include the actual transport as well as those activities such as eleasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport authorized transport and courier personnel may include individuals from outside the organization (e.g. U.S. Postal Service or a commercial transport or de ivery serv ce). Maintaining accountabi ity of med a during transport includes for examp e restricting transport activ ties to authorized personnel and tracking and/or obtaining explicit ecords of transport activities as the media moves through the transportation system to prevent and detect loss destruct on or tampering. Organ zations establish documentat on requirements for activ ties associated with the transport of information system med a in accordance with organizational assessments of risk to include the flexibi ity to define different record-keeping methods for the d fferent types of media transport as part of an overall system of transport-re ated records.
Med a P otect on	3.8.6	Implement c yptog aph c mechan sms to p otect the conf dent al ty of CUI sto ed on d g tal med a du ng t ansp t unless othe w se p otected by a te hat ve phys cal safegua ds. *** Rev 3, W thd awn Inco po ated nto 3.8.5. *****		No		No c yptog aph c mechan sms a e n place fo CUI sto ed on d g tal med a du ng t ans t. Laptops a e enc ypted, othe fo ms of d g tal sto age a e not. The e a e gene al data p otect on pol c es and p ocedu es fo cont o l ng SGI.	None
Med a P otect on	3.8.7	Cont ol the use of emovable med a on system components.		No		No emovable med a cont ols a e n place. When a new USB has been connected to a company laptop, the USB w ll be enc ypted and cont olled by a passwo d. The emovable med a s not t acked a cont olled by an ex st ng pol cy.	Information system media includes both digital and non-dig tal media. Dig tal media includes for example diskettes magnetic tapes external/removab e hard disk drives flash drives compact d sks and d gital video disks. Non-digital med a includes for examp e paper and microfilm. This control a so applies to mobi e devices with informat on sto age capability (e.g. smart phones tablets E-readers). In contrast to MP-2 (See NIST SP800 53 R4) which restricts user access to media th s control restr cts the use of certain types of media on information sys ems for example restr cting/prohib ting the use of flash drives or external hard disk drives. Organizat ons can employ technical and nontechnical safeguards (e.g. pol cies procedures rules of behavio) to restrict the use of information system med a. O gan zations may restrict the use of portab e storage devices for example by using physical cages on workstations to prohibit access to certain external ports or disabling/removing the ability to insert read or write to such devices. Organizations may a so limit the use of portable storage devices to only approved devices including for example dev ces prov ded by the organization devices provided by other approved organizat ons and devices that are not personally owned. Fina ly organizations may restrict the use of portab e storage devices based on the type of dev ce for example prohibiting the use of wri eable portab e storage devices and imp ementing this restriction by d sabling or removing the capabi ity to write to such devices.
Med a P otect on	3.8.8	P oh b t the use of po table sto age dev ces when such dev ces have no dent f able owne . *** Rev 3, . W thd awn Inco po ated nto 3 8 7.******		No		Use s do not have to be dent f able owne s of po table sto age.	Requiring ident fiable owners (e g. individuals organizations or projects) for portable storage dev ces reduces the r sk of using such technologies by allowing organizations to assign responsibil ty and accountability for addressing known vulnerabil ties in the dev ces (e.g. malicious code insertion).
Phys cal and Env onmental P otect on	3.10.6	Enfo ce safegua d ng measu es fo CUI at a te nate wo k s tes.		No		No p ocedu es fo cont o l ng CUI. The e a e gene al data p otect on pol c es and p ocedu es fo cont oll ng SGI. Phys cal secu ty w l cont ol ans enfo ce safegua d ng measu e at alte nate wo k s tes.	A ternate work sites may include for examp e government facil ties or private residences of employees. Wh le commonly distinct from alternative processing s tes a ternate work sites may provide eadily avai ab e alte nate ocations as part of contingency operat ons. Organizat ons may define different sets of secur ty controls for specific a ternate work sites or types of sites depending on the work related activ ties conducted at those s tes. This control supports the con ingency planning activities of o gan zations and the federal telework in tiative.
R sk Assessment	3.11.1	Pe od cally assess the sk to o gan zat onal ope at ons (ncludi ng m ss on, funct ons, mage, o eputat on), o gan zat onal assets, and nd v duals, esult ng f om the ope at on of o gan zat onal systems and the assoc ated p ocess ng, sto age, o t ansm ss on of CUI.				Cove ed when CUI becomes pa t of Ente gy Data P og am.	C early defined authorizat on boundaries are a pre equis te for effective risk assessments. Risk assessments take into account threats vulnerab lit es likelihood and impact to organ za ional operations and assets individua s other organ zations and the Nation based on the operation and use of information systems. Risk assessments also take into account risk from external part es (e.g. service providers contractors operating information sys ems on beha f of the organization indiv duals accessing organizational information systems outsourcing ent ties). In accordance w th OMB policy and re ated E-authent cat on init atives authent cat on of publ c users accessing federal information systems may also be required to protect nonpubl c or privacy-re ated information. As such organizational assessments of r sk a so address publ c access to federal informat on systems. Risk assessments (either formal or info mal) can be conducted at a l th ee tiers in the risk management hierarchy (i.e. organization level miss on/business process level or information system leve) and at any phase in the system development ife cycle. R sk assessments can also be conducted at various steps in the R sk Management Framework including categorizat on security control selection security control implementat on security control assessment information system authorization and security control mon toring. RA-3 s notewo thy in that the control must be partially implemented prior to the implementation of other controls in order o complete the first two steps in the Risk Management Framework. Risk assessments can play an important role in secu ity control selection processes particularly during the app ication of tailoring guidance which includes security control supp ementation.

System and Commun cat ons P otect on	3.13.11	Employ FIPS-val dated c yptog aphy when used to p otect the conf dent al ty of CUI.		FIPS-val dated c yptog aphy s not used	Cryptography can be emp oyed o support a variety of secu ity solutions including for example the protection of classif ed and Control ed Unc assified Information the provision of dig tal signatu es and the enforcement of information separation when authorized indiv dua s have the necessary clearances for such information but ack the necessary formal access approva s. Cryp ography can also be used to support random number generation and hash generation. Generally app icable cryptographic standards include FIPS-va idated 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 ect on of other secur 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 d gital s gnatures FIPS-va idated cryptography).
System and Commun cat ons P otect on	3.13.12	P oh b t emote act vat on of collabo at ve comput ng dev ces and p ov de nd cat on of dev ces n use to use s p esent at the dev ce.		Collabo at ve comput ng s allowed fo emote access to p ov de ma ntenance suppo t fo systems w thout a use to be phys ca ly p esent at the dev ce.	NIST 800-53 R4 defines this control as follows Control The informat on system a. Prohib ts remote activat on of collaborative computing devices with the fo lowing except ons [Assignment organization-defined except ons where remote activation s to be a lowed] and b. Provides an expl cit indication of use to users physically present at the devices. Supp emental Collaborative computing dev ces include for example networked white boards cameras and microphones. Exp ic t indication of use includes for examp e signa s to users when collaborative computing devices are activated.