From: [redacted] via 800-171comments
To: 800-171comments@list.nist.gov
Cc: [redacted]
Subject: [800-171 Comments] Comments on NIST SP 800-171r3 initial public draft
Date: Friday, July 14, 2023 11:53:46 PM
Attachments: image001.png
sp800-171r3-ipd-comment-template.xlsx

Dear Dr. Ross and Ms. Pillitteri,

Thank you for the opportunity to weigh in on NIST SP 800-171 Rev 3. Despite the large number of comments in the attached, we feel that Rev 3 is a great step forward and appreciate all of the effort you put into it. If there is an opportunity assist NIST in the Rev 3 or other, related efforts, or if any of the comments are "less than clear", please do not hesitate to reach out.

Best Regards,

- Jim

James Goepel
Co-Founder
CMMC Information Institute
A nonprofit educational organization
[redacted]
https://www.CMMCInfo.org

Comment #	Submitted By (Name/Org) *	Type (General / Editorial / echnical)	Source (publication analysis overlav)	Starting Page # *	Starting Line #*	Comment (nclude rationale)*	Suggested Change*
1	Fe nando Machado / Cybe sec Investments	Ed to al	F equently Asked Quest ons	2	Unknow n	In the 'F equently Asked Quest ons In t al Publ c D aft (PD) N ST SP 800-171, Rev s on 3 document unde quest on 'Why d d NIST nt oduce o gan zat on- def ned pa amete s (ODP) n selected secu ty equ ements?' t states, Fede al agenc es can elect to spec fy ODP's, p ov de gu dance on select ng ODP's fo nonfede al agenc es, o allow nonfede al agenc es to se f-select ODP values.	I suggest NIST def ne the te m 'nonfede al agency' o co ect to state 'nonfede al o gan zat on' as def ned n the NIST SP 800-171 Glossa y.
2	CMMC Info mat on Inst tute	Gene al	Publ cat on	N/A	N/A	The d scuss on of the elat onsh p w th 800-53 s g eat, but fo most of those who w l ead th s document, t s elevant. Wh le NIST SP 800-171 may have n t ally been w tten to a d gove nment agenc es n establ sh ng equ ements fo p otect ng CUI n nonfede al systems, the eal ty s that 32 CFR 2002 establ shes th s publ cat on as the bas s fo p otect ng CUI. Thus, agency pe sonnel a e la gely gno ant to ts equ ements. Instead, t s passed, n whole, to gove nment cont acto s and othe nonfede al ent t es. NIST should the efo e take th s add t onal aud ence nto account n Rev 3. Fo example, the vast majo ty of the nonfede al ent t es w ll neve have hea d of, let alone have ead, NIST SP 800-53. But they MIGHT have hea d of the NIST CSF. NIST should nclude language, o a po nte to anothe document, that desc bes how/whe e NIST SP 800-171 f ts n w th othe contextually- elevant NIST publ cat ons l ke the NIST CSF, N ST SP 800-30/37/39, FIPS 140, F PS 199, FIPS 200, etc.	
3	CMMC Info mat on Inst tute	Gene al	Publ cat on	N/A	N/A	If NIST would l ke ass stance w t ng such a document, we would be glad to ass st.	
4	CMMC Info mat on Inst tute	Gene al	Publ cat on	N/A	N/A	N ST must ecogn ze that th s publ cat on w ll make o b eak ca ee s, cause gove nment cont acto s to ex t the gove nment cont act ng ma ket, and even cause false cla ms and othe legal l ab l ty fo cont acto s. The efo e, cons stency, cla ty, and p ec s on a e mpo tant as pa t of the ev sed publ cat on and the ev s ons to NIST SP 800-171A. Fo example, when a nonfede al ent ty s equ ed to pe fo m an act, the only p ope modal ve bs to use when desc b ng the equ ement a e must o shall . Othe ve bs such as should , can , and may a e pe m ss ve and the efo e do not c eate equ ements. NIST's use of expected w th espect to the NFO cont ols c eates s m la ssues. That ve b s gene ally pe m ss ve (t s def ned as ega ded as l kely ant c pated , and the efo e not equ ed), yet ead n context the desc pt on of the NFO cont ols could be ead as though NIST assumes they a e n place, mak ng them a equ ement. Th s amb gu ty w ll lead to l t gat on that w ll h nde the adopt on of NIST SP 800-171 ac oss nonfede al agenc es. NIST should the efo e avo d the use of amb guous te ms such as expected and mo e clea ly def ne whethe o not the NFO cont ols a e equ ed.	
4	CMMC Info mat on Inst tute	Gene al	Publ cat on	N/A	N/A	N ST should establ sh a sco ng app oach that allows agenc es to cont ast the ove all cybe secu ty matu ty of two d ffe ent nonfede al ent t es when those agenc es a e mak ng p ocu ement dec s ons. Examples nclude DoD's Assessment Methodology and the FAR and Above methodology developed by the CMMC Info mat on Inst tute and used by thousands of o gan zat ons who have downloaded and use ou f ee self-assessment tool/sp eadsheet. We would be happy to sha e the nfo mat on w th NIST as and when app op ate.	
5	CMMC Info mat on Inst tute	Gene al	Publ cat on	N/A	N/A	N ST should establ sh ecommended gap analys s and emed at on p o t es fo the va ous cont ols. Fo example, many nonfede al ent t es w l beg n w th 3.1.1, wh ch s full of complex concepts and tends to be ve y nt m dat ng. Recommend ng that the ent t es beg n the gap analyses w th the phys cal secu ty and pe sonnel secu ty doma ns would allow them to beg n w th mo e st a ghtfo wa d concepts and would l kely make the p ocess much eas e . Establ sh ng a ecommended POA&M emed at on o de would also s gn f cantly benef t nonfede al ent t es. The CMMC Info mat on Inst tute has publ shed both ecommended gap analys s and POA&M emed at on o de s unde C eat ve Commons l censes and would be happy to sha e them w th N ST as and when app op ate.	
6	CMMC Info mat on Inst tute	Ed to al	Publ cat on	N/A	N/A	Most eade s a e p ck ng up the document because t shows up as a equ ement n a cont act. They w l be unfam l a w th CUI, compl ance, laws, and many othe top cs. The Abst act s the ve y f st th ng eade s w ll see. They need mo e context than what s he e, even fo an abst act. Yes, they can ead fu the nto the document to get some of the nfo mat on, but you' e speak ng past them. St ongly ecommend add ng mo e context, along the l nes of what s n the Suggested Change.	We ecommend updat ng the nt oduct on to ead along the l nes of the follow ng Cont olled Unclass f ed Info mat on ("CUI") s nfo mat on that a law, egulat on, o gove nment-w de pol cy equ es o pe m ts the use of safegua d ng and/o l m ted d ssem nat on cont ols. The safegua d ng of CUI s of pa amount mpo tance to ou nat on and can d ectly mpact the ab l ty of the fede al gove nment to successfully conduct ts essent al m ss ons and funct ons. Fede al agenc es a e enhanc ng the own CUI safegua d ng effo ts to meet the co espond ng legal and egulato y equ ements when the CUI s c eated by fede al agenc es o sto ed n fede al systems. Fede al agenc es must also ensu e CUI s p ope ly safegua ded when t s d ssem nated to, o c eated unde fo the fede al gove nment unde cont act w th, nonfede al ent t es. Nonfede al ent t es nclude nd v duals and o gan zat ons such as, w thout l m tat on, gove nment cont acto s, state and local gove nment agenc es, and fo e gn gove nments. To mp ove eff c ency and educe the bu den on those nonfede al ent t es, Cong ess and the Wh tehouse tasked NIST w th establ sh ng the ecommended m n mum secu ty equ ements app op ate to p otect CUI n nonfede al systems. Th s publ cat on sets fo th those m n mum ecommended secu ty equ ements. NIST SP 800-171A def nes the ecommended assessment object ves and techn ques that a e used to evaluate whethe a nonfede al ent ty meets a pa t cula safegua d ng equ ement def ned n th s publ cat on. Nonfede al ent t es a e encou aged to ca efully ev ew NIST SP 800-171A as they def ne the secu ty and compl ance p og ams. The safegua d ng equ ements n th s publ cat on apply to all components of nonfede al systems that p ocess, sto e, o t ansm t CUI o that p ov de p otect on fo such components. 32 CFR 2002.14(h)(2) establ shes th s publ cat on as the m n mum set of secu ty equ ements necessa y to p otect CUI Bas c nfo mat on on a l appl cable systems, except whe e such systems a e collect ng o ma nta n ng nfo mat on on behalf of a fede al agency o us ng o ope at ng a system on behalf of an agency. The safegua d ng equ ements n th s publ cat on a e ntended fo use by fede al agenc es n cont actual veh cles o othe ag eements establ shed between those agenc es and nonfede al ent t es. Nonfede al ent t es wh ch handle CUI Spec f ed nfo mat on should consu t w th the d ssem nat ng agency to dete m ne the add t onal safegua d ng equ ements fo that CUI. Fo mo e nfo mat on about the CUI p og am and the d st nct ons between CUI Bas c and CUI Spec f ed nfo mat on, v s t https //a ch ves.gov/CUI.
7	CMMC Info mat on Inst tute	Ed to al	Publ cat on	N/A	N/A	N ST should c eate a table of all ODPs, ensu e they a e nd v dually efe enceable, and dedupl cate them fo cons stency.	N/A
8	CMMC Info mat on Inst tute	Ed to al	Publ cat on	N/A	N/A	The po nt of N ST SP 800-171 s to p otect CUI. The language th oughout the publ cat on should, the efo e, be cons stent w th the concepts embod ed n the CUI p og am (.e., EO 13556 and 32 CFR 2002). In many cases, the language s o ented a ound systems and oles, athe than the CUI and the natu e of the CUI. Fo example, as d scussed below, some cont ols focus on need to know , wh ch s not the ght standa d fo establ sh ng d ssem nat on autho ty, and othe s focus on l m t ng access by ole (wh ch suggests o gan zat on ole, such as eng nee ng manage) but not all pe sons n a pa t cula ole w ll have a lawful gove nment pu pose to access pa t cula CUI.	CUI-o ented concepts f om 32 CFR 2002 and EO 13556 should be adopted and nco po ated th oughout the publ cat on.
9	CMMC Info mat on Inst tute	Ed to al	Publ cat on	1	21	It s unclea f om the text whethe these bullets a e ntended to be o ned by an and o an o .	We ecommend add ng the app op ate conjunct on at the end of the second bullet (most l kely and).
10	CMMC Info mat on Inst tute	Ed to al	Publ cat on	1	22	32 CFR 2002.14(h)(2) states NIST SP 800–171 (nco po ated by efe ence, see § 2002.2) def nes the equ ements necessa y to p otect CUI Bas c on non-Fede al nfo mat on systems n acco dance w th the equ ements of th s pa t. Th s establ shes NIST SP 800-171 as the basel ne fo p otect ng CUI Bas c. That makes the equ ements n the publ cat on mo e than me ely ecommendat ons . They a e equ ements that all nonfede al ent t es must meet when handl ng CUI.	We ecommend eph as ng The pu pose of th s publ cat on s to p ov de fede al agenc es w th ecommended secu ty equ ements… to ead The pu pose of th s publ cat on s to p ov de fede al agenc es w th secu ty equ ements…
11	CMMC Info mat on Inst tute	Ed to al	Publ cat on	2	27	The way th s bullet s ph ased, t sounds as though, f a law, egulat on, o gove nment-w de pol cy c eates CUI Spec f ed nfo mat on, the equ ements n NIST SP 800-171 no longe apply to that nfo mat on and the nfo mat on must only be p otected as spec f ed n the law, egulat on, o gove nment-w de pol cy. That s not t ue. Othe w se, fo example, nfo mat on that was des gnated as CUI unde 49 CFR 1520.11 would not be sub ect to the majo ty of the safegua d ng equ ements unde th s publ cat on. That s s mply log cal and ncons stent w th the ntent of the CUI p og am. Instead, the equ ements n the co espond ng law, egulat on, o gove nment-w de pol cy supplement and, n the event of a confl ct, eplace those n NIST SP 800-171.	We ecommend eph as ng th s to ead Except and only to the extent that a law, egulat on, o Gove nment-w de pol cy l sted n the CUI eg st y fo the CUI catego y o subcatego y of nfo mat on p esc bes spec f c safegua d ng equ ements fo p otect ng the nfo mat on's conf dent al ty.
12	CMMC Info mat on Inst tute	Ed to al	Publ cat on	2	31	The emphas zed o n th s sentence c eates confus on.	We ecommend eplac ng the o w th as we l as
13	CMMC Info mat on Inst tute	Ed to al	Publ cat on	3	70	As d scussed above, expected s an amb guous te m and c eates unce ta nty that could have a s gn f cant mpact on the adopt on of NIST SP 800-171 by nonfede al ent t es.	f N ST ntends the cont ols to be n place, th s should be mo e expl c t. Fo example, th s could be eph ased as Expected to always be mplemented by nonfede al o gan zat ons w thout spec f cat on by the Fede al Gove nment , o Always n place n nonfede al o gan zat ons w thout spec f cat on by the Fede al Gove nment , o Requ ed fo p otect on of a l nfo mat on and the efo e mplemented w thout spec f cat on by the Fede al Gove nment . Howeve , the bette app oach would be to nco po ate the NFO cont ols nto N ST SP 800-171 f they a e actually equ ed.
14	Fe nando Machado / Cybe sec Investments	Ed to al	Publ cat on	4	79	L ne 79 states, These ODP's p ov de add t onal flex b l ty by allow ng fede al o gan zat ons to spec fy values fo the des gnated pa amete s, as needed.	I suggest co ect ng to state fede al o nonfede al o gan zat ons' s nce the NIST SP 800-171 document s focused on the p otect on of cont o led unclass f ed nfo mat on n nonfede al systems and o gan zat ons.
15	CMMC Info mat on Inst tute	Gene al	Publ cat on	4	79	N ST should p ov de add t onal nfo mat on about wh ch o gan zat on should def ne the ODPs. A e these left fo the nonfede al ent t es to dete m ne, o should they be set by the agency?	
16	CMMC Info mat on Inst tute	Gene al	Publ cat on	4	79	N ST should establ sh ecommended ODP values o anges of values. Cu ently, the e s s gn f cant amb gu ty as to what s equ ed, and that leaves a lot of d sc et on to the agenc es o non-fede al ent t es. Gu dance f om NIST would help establ sh mo e cons stency, educe the ove all bu den fo the nonfede al ent t es, and u t mately educe the cost and sk to taxpaye s to p otect CUI.	
17	Fe nando Machado / Cybe sec Investments	Ed to al	Publ cat on	5	113	L ne 113 states, When used n the context of the equ ements n Sect on 3, the te m system means a nonfede al system that p ocesses, sto es, o t ansm ts CUI.	I suggest nco po at ng Pa ag aph 1.1 Pu pose and Appl cab l ty statement (l ne 30) The secu ty equ ements n th s publ cat on a e only appl cable to components of nonfede al systems that p ocess, sto e, o t ansm t CUI o that p ov de p otect on fo such components.
18	CMMC Info mat on Inst tute	Gene al	Publ cat on	5	120	The pu pose of NIST SP 800-171 s to p otect CUI. The language n the publ cat on should the efo e be mo e cons stent w th 32 CFR 2002 and EO 13556. Fo example, we ecommend ty ng the autho zed accounts to nd v duals w th lawful gove nment pu pose to access the spec f c CUI handled by that system. The d scuss on should nclude a cla f cat on that nd v duals w th a lawful gove nment pu pose to access ce ta n CUI on one system may not have a lawful gove nment pu pose to access d ffe ent CUI on that same system.	
19	CMMC Info mat on Inst tute	Ed to al	Publ cat on	5	137	Th s equ ement efe ences need-to-know , but that s not the p ope standa d fo analyz ng whethe autho zat on st ll ex sts. Unde 32 CFR 2002, the standa d s lawful gove nment pu pose .	We ecommend eph as ng th s to add ess When system usage changes o the nd v dual no longe has a lawful gove nment pu pose to access spec f c CUI.
20	CMMC Info mat on Inst tute	Ed to al	Publ cat on	6	152	The te m suppo t s used th oughout the publ cat on to efe to p ov d ng b eak/f x and othe ma ntenance se v ces. The use of that same wo d n the ph ase …to suppo t t avel equ ements). could c eate confus on n the m nd of the eade .	We ecommend eplac ng …to suppo t t avel equ ements w th …to fac l tate t avel equ ements
21	CMMC Info mat on Inst tute	Ed to al	Publ cat on	9	296	G ammat cal ssue	Add a comma afte …lockouts a e .

Comment #	Submitted By (Name/Org) *	Type (General / Editorial / echnical)	Source (publication analysis overlav)	Starting Page # *	Starting Line #*	Comment (nclude rationale)*	Suggested Change*
22	CMMC Info mat on Inst tute	Ed to al	Publ cat on	12	419	The use of the ph ase o gan zat on-cont olled mob le dev ces suggests that t s OK to have CUI on non-cont olled mob le dev ces.	We ecommend eph as ng th s to ead a. Establ sh conf gu at on equ ements, connect on equ ements, and mplementat on gu dance wh ch allow the o gan zat on to p otect and manage the conf dent al ty of CUI on mob le dev ces. b. L m t access to the system to only o gan zat on-autho zed mob le dev ces on wh ch the establ shed conf gu at on equ ements, connect on equ ements, and mplementat on gu dance has been mplemented and on wh ch the o gan zat on can exe t cont ol ove CUI. c. Implement [Select on full-dev ce enc ypt on conta ne -based enc ypt on] to p otect the conf dent al ty of CUI on mob le dev ces.
23	CMMC Info mat on Inst tute	Ed to al	Publ cat on	14	485	The way th s equ ement s ph ased, t sounds as though the nonfede al ent ty s expected to have cont ol ove the exte nal system and the ab l ty to plug emovable med a nto that exte nal system. In most cases, that s not t ue.	Th s equ ement should be eph ased to cla fy that th s s spec f c to the aspects of the exte nal system that the ent ty has cont ol ove .
24	CMMC Info mat on Inst tute	Ed to al	Publ cat on	14	501	Th s s awkwa dly ph ased.	We ecommend sho ten ng th s to T a n autho zed nd v duals to dent fy CUI.
25	CMMC Info mat on Inst tute	Gene al	Publ cat on	15	524	The t a n ng fam ly should nclude a equ ement fo t a n ng elated to CUI des gnat on, ma k ng, d ssem nat on, and safegua d ng.	
26	CMMC Info mat on Inst tute	Gene al	Publ cat on	18	662	Th s should be augmented to nclude a gove nance component. The ale ts themselves a e g eat, but the e needs to be follow-up act on f the ale t o esponse sn't add essed n a t mely manne .	We ecommend eph as ng along the l nes of a. Ale t [Ass gnment o gan zat on-def ned pe sonnel o oles] w th n [Ass gnment o gan zat on-def ned t me pe od] n the event of an aud t logg ng p ocess fa lu e. b. Take the follow ng add t onal act ons [Ass gnment o gan zat on-def ned add t onal act ons]. c. Log the act ons taken. d. Ale t [Ass gnment o gan zat on-def ned pe sonnel o oles] f the add t onal act ons a e not taken w th n [Ass gnment o gan zat on-def ned t me pe od].
27	CMMC Info mat on Inst tute	Gene al	Publ cat on	29	1069	Many o gan zat ons a e mov ng away f om passwo ds to passwo dless systems. NIST should establ sh ecommendat ons and equ ements fo the mplementat on of such systems.	
28	CMMC Info mat on Inst tute	Ed to al	Publ cat on	29	1074	G ammat cal ssue	S nce the concept of a l st of commonly-used, expected, o comp om sed passwo ds has not been nt oduced, ...on the l st of... should be ...on an o gan zat onally-ma nta ned l st of... . The equ ement should also be augmented to nclude pe od c updates to that l st at o gan zat onally-def ned nte vals.
29	CMMC Info mat on Inst tute	Ed to al	Publ cat on	32	1207	Although the o gan zat on s equ ed to pe od cally ev ew and update the t a n ng content, the way th s equ ement s ph ased, the o gan zat on only eve needs to t a n ng the system use s once. The equ ement should be augmented to nclude an ODP fo how often et a n ng should occu .	We ecommend eph as ng th s to ead a. P ov de nc dent esponse t a n ng to system use s cons stent w th ass gned oles and espons b l t es at least [Ass gnment o gan zat on-def ned f equency]. B. Rev ew and update nc dent esponse t a n ng content [Ass gnment o gan zat on-def ned f equency] and follow ng [o gan zat on-def ned events].
30	CMMC Info mat on Inst tute	Ed to al	Publ cat on	35	1310	Unde 32 CFR 2002, access to CUI s to be l m ted to those w th a lawful gove nment pu pose, not me ely a spec f c ole. Fo example, an eng nee ng manage on one p oject may not have a lawful gove nment pu pose to access CUI f om anothe p oject. The efo e, I m t ng access to spec f c o gan zat on oles (e.g., eng nee ng manage s) w ll not meet the equ ements of 32 CFR 2002. Th s equ ement should be eph ased to focus on those w th a lawful gove nment pu pose.	We ecommend eph as ng th s equ ement to ead, fo example Rest ct access to CUI on d g tal and non-d g tal med a to nd v duals w th a lawful gove nment pu pose to access that CUI.
31	CMMC Info mat on Inst tute	Ed to al	Publ cat on	36	1339	32 CFR 2002 equ es that a l med a conta n ng CUI be ma ked. G ant ng an exempt on s ncons stent w th th s equ ement.	3.8.4 b. should be emoved.
32	CMMC Info mat on Inst tute	Ed to al	Publ cat on	36	1352	G ammat cal ssue	We ecommend eph as ng ...CUI and du ng t anspo t... to ead ...CUI nclud ng du ng t anspo t...
33	CMMC Info mat on Inst tute	Ed to al	Publ cat on	38	1430	When an nd v dual s eass gned o t ansfe ed to othe pos t ons n the o gan zat on, the o gan zat on should eevaluate whethe that nd v dual st ll has a lawful gove nment pu pose to access the CUI to wh ch they have access. Thus, the analys s sn't s mply l m ted to cu ent log cal and phys cal autho zat ons to the system and fac l ty .	We ecommend eph as ng th s equ ement to add ess the lawful gove nment pu pose equ ement. Fo example 1. Rev ew and conf m the ongo ng ope at onal need fo cu ent log cal and phys cal access autho zat ons to the system and fac l ty, and a lawful gove nment pu pose to access the CUI conta ned the e n.
34	CMMC Info mat on Inst tute	Ed to al	Publ cat on	39	1475	Unde 32 CFR 2002, autho zed access should be l m ted to those w th a lawful gove nment pu pose. Mak ng th s mo e expl c t n the equ ement w ll make t eas e fo nonfede al ent t es to ensu e they a e meet ng the ntent of 32 CFR 2002.	We ecommend eph as ng th s equ ement to ead Develop, app ove, and ma nta n a l st of nd v duals who have a lawful gove nment pu pose and a e autho zed to access the fac l ty whe e the CUI es des.
35	CMMC Info mat on Inst tute	Ed to al	Publ cat on	39	1475	Th s equ ement focuses on whe e the "system" es des, but n footnote 3, system s def ned as only the d g tal aspects. Phys cal secu ty equ ements also apply whe e non-d g tal CUI s sto ed.	We ecommend eph as ng ...whe e the system es des. to "...whe e the CUI es des."
36	CMMC Info mat on Inst tute	Gene al	Publ cat on	41	1530	N ST needs to add mo e def n t on he e. We know MANY people w ll be wo k ng f om home. What phys cal secu ty equ ements need to be n place? What othe equ ements must be mplemented? G ven ts p evalence, N ST should cons de c eat ng a new doma n that s focused on emote wo k.	
37	CMMC Info mat on Inst tute	Ed to al	Publ cat on	41	1541	Keys and comb nat ons a e not phys cal access dev ces. They a e used to unlock/ope ate the phys cal access dev ces.	We suggest eph as ng th s to "Secu e keys, comb nat ons, and othe dent f e s used to cont ol the ope at on of phys cal access dev ces."
38	CMMC Info mat on Inst tute	Gene al	Publ cat on	42	1590	Most gove nment cont acto s a e not fam l a w th sk assessments. In the p ev ous pa ag aph (l ne 1583), NIST desc bes sk assessments as cons de ng th eats, vulne ab l t es, l kel hood, and mpact. Yet n l ne 1590, NIST nt oduces the dea of a "supply cha n event" w thout def n ng what th s s o means. Is an event the same th ng as a th eat? Is t the occu ence of a th eat (.e., an nc dent)? O someth ng else? If someth ng else, should that be ncluded n the l st n l ne 1583?	
39	CMMC Info mat on Inst tute	Ed to al	Publ cat on	43	1600	The way th s s ph ased, t sets up o gan zat ons to fa l assessments. How does the o gan zat on meet the "and when new vulne ab l t es affect ng the system a e dent f ed" equ ement? If the e s any lag at a l between when a new vulne ab l ty s announced and when the scan s pe fo med, the o gan zat on s not compl ant.	We ecommend nclud ng and ODP that allows fo a easonable pe od of t me. Also need to desc be n the d scuss on how/whe e o gan zat ons can go to get nfo mat on on when new vulne ab l t es a e dent f ed.
40	CMMC Info mat on Inst tute	Ed to al	Publ cat on	43	1627	Must the scann ng tools automat cally t gge e-scans eve y t me a new vulne ab l ty s announced? Th s could have a s gn f cant mpact on system pe fo mance, etc. Espec ally f those tools scan eve y dev ce on the netwo k.	We ecommend eph as ng to nclude a d scuss on of the potent al mpact and the facto s a nonfede al ent ty should use when evaluat ng the f equency/t gge s fo escann ng.
41	CMMC Info mat on Inst tute	Ed to al	Publ cat on	44	1639	The way th s s ph ased, t sets up o gan zat ons to fa l assessments. The e sn't any t me pe od, wh ch suggests that the esponse must be nstantaneous.	We ecommend add ng ODPs wh ch allow the nonfede al ent ty to espond n d ffe ent t me pe ods based on the seve ty of the f nd ngs.
42	CMMC Info mat on Inst tute	Gene al	Publ cat on	44	1653	Unless assessment esults a e epo ted to, and s gned off on by, sen o management, ssues that a e dent f ed can be h dden by employees.	We ecommend add ng a equ ement that all assessment esults, nclud ng nte nal and th d-pa ty assessments, and the co espond ng POA&Ms be epo ted to and s gned off by a sen o execut ve of the o gan zat on (.e., a membe of the C-su te o Boa d of D ecto s).
43	CMMC Info mat on Inst tute	Gene al	Publ cat on	45	1681	POA&Ms should have m lestones w th n a easonable pe od of t me.	We ecommend establ sh ng ODPs that set max mum pe ods of t me fo mplementat on of all m lestones (e.g., 24 to 36 months) based on seve ty o othe met cs.
44	CMMC Info mat on Inst tute	Ed to al	Publ cat on	45	1701	Cont nuous s a dange ous wo d. In the Oxfo d Languages d ct ona y, cont nuous s def ned as fo m ng an unb oken whole w thout nte upt on . The efo e, any pause o b eak, whethe ntent onal o not, could be g ounds fo the nonfede al ent ty to fall out of compl ance. Wh le NIST appea s to be attempt ng to m t gate the sk of such ssues by stat ng that the ...te ms cont nuous and ongo ng mply that o gan zat ons assess and mon to the cont ols and sks at a f equency suff c ent to suppo t sk-based dec s ons , these mpl cat ons may not be legally suff c ent fo nonfede al ent t es to avo d false cla ms act and othe l ab l ty.	We ecommend that NIST fo mal ze the def n t ons of cont nuous and ongo ng f om the d scuss on and move them nto the glossa y.
45	CMMC Info mat on Inst tute	Ed to al	Publ cat on	46	1716	The ndependent assessment equ ement s a welcome add t on to NIST SP 800-171. We st ongly concu that th s should be a fundamental pa t of all CUI compl ance p og ams. Howeve , th s equ ement needs mo e spec f c ty.	We ecommend that NIST add ODPs wh ch def ne how often the ndependent assessment should be conducted, wh ch nd v duals/ent t es a e autho zed to conduct such assessments, and wh ch cont ols must (and should) be assessed (e.g., only those n NIST SP 800-171, o must othe cont ols also be assessed?).
46	Fe nando Machado / Cybe sec Investments	Ed to al	Publ cat on	46	1717	L ne 1717 states, Use ndependent assesso s o assessment teams to assess cont ols.	I suggest establ sh ng an [ass gnment o gan zat on-def ned f equency] s nce t s not clea how often ndependent assessments a e to be conducted.
47	CMMC Info mat on Inst tute	Gene al	Publ cat on	46	1731	Unde 32 CFR 2002 16(a)(4), an autho zed holde can only d ssem nate CUI to someone else when the autho zed holde has a easonable bel ef that the ntended ec p ent s also an autho zed holde (.e , they have a lawful gove nment pu pose to access the CUI and they a e not excluded f om access ng t by a l m ted d ssem nat on cont ol on the CUI), AND the autho zed holde must have a easonable bel ef that the ntended ec p ent knows how to handle CUI.	We ecommend eph as ng the nfo mat on exchange equ ement to mo e expl c tly efe ence the equ ements def ned n 32 CFR 2002, nclud ng the autho zed holde and knowledge equ ements.
48	CMMC Info mat on Inst tute	Ed to al	Publ cat on	46	1731	Wh le most nfo mat on s exchanged n d g tal o elect on c fo m these days, the e a e ce ta n ndust es n wh ch s gn f cant quant t es of CUI s st ll exchanged on pape . As noted above, footnote 5 def nes a system as the d g tal/elect on c aspects of an o gan zat on. Th s equ ement's emphas s on the exchange of CUI between systems the efo e leaves a gap n the p otect on of pape -based CUI.	We ecommend eph as ng th s equ ement to add ess both systems wh ch sha e nfo mat on and the exchange of pape based CUI between autho zed holde s.
49	CMMC Info mat on Inst tute	Ed to al	Publ cat on	51	1916	Wh le we ag ee that the FIPS-val dat on equ ements n NIST SP 800-171 Rev. 2 a e ove ly st enuous and often lead to nonfede al ent t es st uggl ng to balance the need fo compl ance aga nst the need to patch the systems to add ess secu ty vulne ab l t es, the equ ements n 3.13 11 sw ng the pendulum too fa n the oppos te d ect on. The way th s s ph ased, t g ves each fede al agency the flex b l ty to def ne acceptable c yptog aphy, but Cong ess has epeatedly nd cated that NIST s the most app op ate agency fo mak ng such dete m nat ons. We a e conce ned that the cu ent language could esult n the autho zat on of h ghly nsecu e enc ypt on modules.	We ecommend amend ng the equ ement to focus on the use of a cu ently FIPS-val dated module o a newe ve s on of that same module that was eleased w th n the p ev ous 24 to 36 months. Th s a lows o gan zat ons the flex b l ty to use newe ve s on of the modules when they a e eleased (and thus add ess ng any known vulne ab l t es), wh le also emov ng the need fo the module develope s to subm t eve y last change to N ST fo eval dat on.
50	CMMC Info mat on Inst tute	Ed to al	Publ cat on	51	1941	Def n t on both acceptable and unacceptable mob le code and mob le code technolog es s a s gn f cant unde tak ng fo small and med um bus nesses.	We ecommend eph as ng th s equ ement to focus on default den al (.e , wh tel st ng) of all mob le code and mob le code technolog es.
51	CMMC Info mat on Inst tute	Gene al	Publ cat on	52	1960	Th s equ ement needs mo e def n t on. It may be p ov ded n NIST SP 800-171A, but, at a m n mum, the d scuss on needs to be enhanced.	
52	CMMC Info mat on Inst tute	Gene al	Publ cat on	53	1994	Th s equ ement needs mo e def n t on. It may be p ov ded n NIST SP 800-171A, but, at a m n mum, the d scuss on needs to be enhanced.	
53	CMMC Info mat on Inst tute	Ed to al	Publ cat on	54	2059	Th s equ ement needs an ODP wh ch def nes the t mef ame n wh ch the ale ts, etc. a e to be gene ated.	We ecommend eph as ng th s equ ement to be s m la to b. Gene ate nte nal secu ty ale ts, adv so es, and d ect ves, as necessa y, w th n [Ass gnment o gan zat onally-def ned f equency].
54	CMMC Info mat on Inst tute	Ed to al	Publ cat on	56	2135	The way th s s ph ased, t suggests that o gan zat ons must w te e the one ove a ch ng pol cy that add esses eve yth ng the o gan zat on does, o pol c es that a e fam ly-spec f c. What about a pol cy that focuses on a spec f c equ ement/cont ol?	We suggest eph as ng th s to ead "...o ep esented by sepa ate pol c es that nd v dual secu ty equ ements o sets/fam l es of secu ty equ ements."
55	CMMC Info mat on Inst tute	Ed to al	Publ cat on	56	2137	Same as above	We suggest eph as ng th s to ead "P ocedu es can be documented n system secu ty plans, n one o mo e sepa ate documents, o as othe w se app op ate
56	CMMC Info mat on Inst tute	Ed to al	Publ cat on	57	2146	The nclus on of ta lo ng act ons as a equ ement n an SSP s p obably a b t much fo most small and med um bus nesses.	We ecommend mov ng the ta lo ng act ons concept to the d scuss on, whe e t can be elabo ated upon and ncluded as pa t of the secu ty equ ements. NIST should also p ov de add t onal gu dance on how to nte p et ta lo ng act ons assessments can be pe fo med p ope ly.
57	CMMC Info mat on Inst tute	Ed to al	Publ cat on	59	2225	Unl ke the gove nment, most cont acto s do not have the ab l ty to fo ce an exte nal p ov de to comply w th the o gan zat on s secu ty equ ements.	We suggest eph as ng th s to focus on establ sh ng a set of secu ty equ ements cons stent w th NIST SP 800-171 (.e , a subset of elevant cont ols) that s then pushed to the cont acto as a fo m wh ch establ shed compl ance, and the acceptance of a th d-pa ty ce t f cat on (f om a t usted th d pa ty such as a C3PAO) as a p oxy fo the complet on of such a fo m.
58	CMMC Info mat on Inst tute	Ed to al	Publ cat on	59	2230	Unl ke the gove nment, most cont acto s do not have the clout o esou ces to allow them to mon to exte nal se v ce p ov de s (e.g , M c osoft, Amazon, etc.) and cont ol the compl ance. Most small gove nment cont acto s w l cont nually fa l to meet th s equ ement f t ema ns n NIST SP 800-171.	Due to ts complex ty, we ecommend emov ng th s equ ement at th s t me. The fede al gove nment should, nstead, encou ag ng ndust y to c eate th d-pa ty p og ams fo val dat ng and epo t ng on compl ance.
59	CMMC Info mat on Inst tute	Ed to al	Publ cat on	59	2252	Th s equ ement focuses on sks to the d g tal system, but the CUI p og am equ es the p otect on of CUI n non-d g tal fo m, too.	Suggest eph as ng/ ef am ng th s to focus on CUI (e.g., Develop a plan fo manag ng supply cha n sks assoc ated w th the development, manufactu ng, acqu s t on, del ve y, ope at ons, ma ntenance, and d sposal of all CUI and systems, system components o system se v ces wh ch handle o secu e CUI), o chang ng the def n t on of "system".
60	CMMC Info mat on Inst tute	Ed to al	Publ cat on	60	2278	Th s equ ement s ove ly b oad. NIST SP 800-171 s des gned to add ess the safegua d ng of CUI, but th s s w tten to add ess a much w de a ay of supply cha n ssues. It s conceptua ly a good dea, but t s outs de of the bounds of NIST SP 800-171.	We suggest eph as ng th s to ead Develop and mplement acqu s t on st ateg es, cont act tools, and p ocu ement methods to p otect aga nst, dent fy, and m t gate supply cha n sks to CUI and to the system, system component(s), o system se v ces wh ch handle o secu e CUI.

Comment #	Submitted By (Name/Org) *	Type (General / Editorial / echnical)	Source (publication analysis overlay)	Starting Page # *	Starting Line #*	Comment (nclude rationale)*	Suggested Change*
61	CMMC Info mat on Inst tute	Ed to al	Publ cat on	60	2301	Th s equ ement s ove ly b oad. NIST SP 800-171 s des gned to add ess the safegua d ng of CUI, but th s s w tten to add ess a much w de a ay of supply cha n ssues. It s conceptua ly a good dea, but t s outs de of the bounds of NIST SP 800-171.	We suggest eph as ng th s to ead a. Estabi sh a p ocess o p ocesses fo dent fy ng and add ess ng weaknesses o def c enc es n the supply cha n elements and p ocesses wh ch handle o secu e CUI. B. Employ [Ass gnment o gan zat on-def ned supply cha n cont ols] to p otect aga nst supply cha n sks to, and l m t the ha m o consequences f om supply cha n elated events to, CUI and the system, system component(s), o system se v ces wh ch handle o secu e CUI.
62	CMMC Info mat on Inst tute	Ed to al	Publ cat on	79	3011	As d scussed above, expected s an amb guous te m and c eates unce ta nty that could have a s gn f cant mpact on the adopt on of NIST SP 800-171 by nonfede al ent t es.	We ecommend eassess ng the app oach to the NFO cont ols.