From:	800-171comments@list.nist.gov on behalf of [redacted]
To:	800-171comments@list.nist.gov
Subject:	[800-171 Comments] Comments on NIST 800-171
Date:	Friday, July 14, 2023 8:55:00 PM
Attachments:	Feedback on 171R3.xlsx

Below comments submitted for your consideration.

I wanted to thank the NIST team for the great, professional job you have done with this. In several instances, I still have serious concerns. You have done a great job of reformatting and adding clarity though. Thank you for your entire team's efforts in this.

W/r
Vince

Vince Scott
CEO and Founder
Defense Cybersecurity Group
[redacted] | Web | Social

Subm tted By	Type	Sou ce	Sta t ng Page #	L ne	Pa a	Comment	Suggested Change
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		25-26	1.1	not collect ng o ma nta n ng nfo mat on on behalf of a Fede al agency. Ou unde stand ng s that unde the cu ent egulat on f we co lect CUI nfo mat on unde a cont act, on ou cont acto netwo k, n acco dance w th 32CFR2002 the p ov s ons of NIST SP 800-171 do apply. Recommend ev s on of th s sentence. The whole language s 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 fo p otect ng the conf dent al ty of CUI When the CUI s es dent n a nonfede al system and o gan zat on When the nonfede al o gan zat on s not co lect ng o ma nta n ng nfo mat on on beha f of a fede al agency o us ng o ope at ng a system on beha f of an agency ---------------------------- So concu w th the f st bullet o us ng o ope at ng a system on behalf of an agency Concu w th the second half of the second bullet.. Th s s the GOCO scene o. But the when the nonfede al o gan zat on s not co lect ng o ma nta n ng nfo mat on on beha f of a fede al agency. It s the not n that pa t of the sentence. Recommend d v d ng the second bullet nto two wh ch I bel eve then ep esents the ntent al gned w th 32CFR2002. - When the nonfede al o gan zat on s co lect ng o ma nta n ng nfo mat on on beha f of a fede al agency - When the nonfede al o gan zat on s not us ng o ope at ng a system on behalf of an agency Th s may be an ed t ng e o whe e the concatonat on of the two ph ases w th o changed the mean ng sl ghtly.	Recommend d v d ng the second bullet nto two wh ch I bel eve then ep esents the ntent al gned w th 32CFR2002. - When the nonfede al o gan zat on s collect ng o ma nta n ng nfo mat on on behalf of a fede al agency - When the nonfede al o gan zat on s not us ng o ope at ng a system on behalf of an agency
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		**31**	**1.1**	**Existing scoping language is interpreted to be overly broad, resulting in all requirements applying to any component providing security functionality (such as NTP servers, log servers, and configurat on management databases) without regard to whether the component could affect the confidentiality of CUI. Suggested change Change "The security requirements in this publication are only applicable to components of nonfederal systems that process, store, or transmit CUI or that provide protect on for such components." to "The security requ rements in this publication are applicable to components of nonfederal systems that process, store, or transm t CUI. Security requirements may be performed by other components in order to protect CUI components.** **The intent of the NIST current language, and renewed emphas s on "or" in revision 3, is to enhance the security of CUI. However, by expanding the scope of applicabil ty NIST is exceeding the r authority under the regulations. NIST has been charged with defininine the security requirements for CUI assets and systems only. As currently worded it opens the door to massive scope expans on for the requirements that is unexecutable. Recommend modification to the language above.**	**Change "The security requirements in th s publication are only applicable to components of nonfederal systems that process, store, or transmit CUI or that provide protection for such components." to "The security requirements in this publ cation are applicable to components of nonfederal systems that process, store, or transmit CUI. Secur ty requirements may be performed by other components in order to protect CUI components."**
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		137	3.1.1	Need-to-know s not the standa d fo access pe 32CFR2002. It s lawful gove nment pu pose. Refe to 32 CFR 2002.16(a)(1)( ). Recommend chang ng the langugage to lawful gove nment pu pose.	Change language to lawful gove nment pu pose
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		148	3.1.1	Recommend nse t ng the wo d may befo e nclude.	Recommend nse t ng the wo d may befo e nclude.
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		166	3.1.2	Cons de whethe the access cont ol pol c es should be [Ass gnment o gan zat ona ly def ned access cont ol pol c es]	Change to ODP
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		181	3.1.3	Cons de f app oved autho zat ons should be [Ass gnment o gan zat onally def ned app oved autho zat ons]	Change to ODP
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		180-209	3.1.3	The d scuss on sect on fo 3.1.3 does not ment on CUI and focuses st ctly on the techn cal aspects of flow cont ol. It s mpo tant fo o gan zat ons to actually cont ol the flow of CUI n o de to p otect ts conf dent al ty, and th s cont ol should nclude a comb nat on of pol cy, p ocedu e, and techn cal flow cont ols that suppo t these pol c es and p ocedu es. Recommend NIST add at least some language n the d scuss on to add ess th s aspect of flow cont ol.	Add language on CUI
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		186	3.1.3	Recommend chang ng expo t-cont olled nfo mat on to CUI. Recommend nse t ng may n f ont of nclude.	Change expo t cont olled to CUI. Inse t may n f ont of nclude.
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		357-385	3.1.12	The e a e cu ently mu t ple d ffe ent def n t ons n the NIST glossa y fo emote access. In pa t cula , Access by use s (o nfo mat on systems) commun cat ng exte nal to an nfo mat on system secu ty pe mete . Sou ce(s) NIST SP 800-82 Rev 2 and Access to an o gan zat onal system by a use (o a p ocess act ng on behalf of a use) commun cat ng th ough an exte nal netwo k. Sou ce(s) NIST SP 800-53 Rev 5. These a e two d ffe ent def n t ons. In the mode n context of comme c al netwo ks gene a ly have components that commun cate us ng exte nal netwo ks. Indeed, we would mag ne that the Fede al Gove nment netwo ks do as well n many ways that a e not obv ous to the system eng nee s and gene ally not cons de ed emote. Any o gan zat on w th mo e than one locat on l kely uses some fo m of exte nal netwo k fo commun cat on even f that s a ded cated leased l ne. F om an OSCs pe spect ve, f a cent al zed IT o gan zat on s access ng pa ts of the system f om a dev ce ns de the system, even f that access t ans ts an exte nal netwo k (a comme c al ISP) t should not be cons de ed emote. Request NIST fo the pu poses of NIST 800-171 Rev 3 adopt the f st def n t on (f om outs de the secu ty pe mete). Th s s a change f om Rev 2, howeve the R2 def n t on d ves emote access cont ols a ound systems and ope at ons that a e effect vely n the wo ld of mode n d st buted comput ng not emote. Th s change would allow these cont ols to (p ope ly and to the benef t of bette secu ty) focus on t uly emote connect on f om outs de the system, to ns de the system, athe than nte nal connect ons that happen to t avel ove f be not owned by the o gan zat on.	Change def n t on to 800-82 def n t on
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		630-631	3.3.2	3.3.2 aud t eco d content. Spec fy ng a phys cal locat on fo whe e an event occu ed w ll be ext emely challeng ng f not mposs ble. Th s nfo mat on can be developed and co elated but hav ng t conta ned n each aud t eco d event s not executable. Recommend st k ng whe e f om the l st of equ ements. L kew se the dent ty of an nd v dual mpacted by an event can equ e co elat ve analys s and s not conta ned n eve y nd v dual eco d. Recommend cla fy ng language that dent fy es that en toto you want to captu e all of these data elements so that th ough analys s when needed you can assessmble the sto y. It s not needed fo each nd v dual logged event to conta n all of these data elements.	St ke whe e f om the l st of equ ements
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		645-646	3.3.3	The comb nat on of 3.3 3b he e w th 3.3.2 def n tely leads to a conclus on that eve y logged event must conta n a l of the data elements l sted. It s necessa y to captu e logs that do NOT conta n a l of these elements because they a e not ava lable at the appl ance do ng the logg ng. If fo assessment pu poses we must show that each event eco d must conta n what type of event occu ed t me whe e sou ce outcome dent ty of an assoc ated nd v dual, subject, object, o ent t es. Locat on and dent ty of a nd v dual a e the most p oblemat c. Aga n th s nfo mat on can be developed f om the total ty of the aud t eco ds/logs howeve cla fy ng language s needed to ensu e th s s not nte p eted by o gan zat ons and assoc ated assesso s that th s means all elements a e equ ed n each eco d.	Inse t qual fy ng language may nclude
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		705-718	3.3.6	Aud t eco d educt on. Does not d ectly mpact p otect ng the conf dent al ty of CUI pa t cula ly the eco d educt on aspect. Recommend emoval. It s a good th ng to have and p ov des afte the fact analyt cal capab l t es to bette exam ne and m ne logs, howeve th s afte the fact capab l ty does not ea ly p otect the conf dent al ty of CUI.	Recommend emoval
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		741-753	3.3.8	Does not d ectly mpact the conf dent al ty of CUI. Recommend emoval.	Recommend emoval
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		754-764	3.3.9	Does not d ectly mpact the conf dent al ty of CUI. Recommend emoval.	Recommend emoval
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		871-872	3.4.6	As w tten seems to say that a l dent f ed po ts, p otocols, and funct ons must be d sabled. In eal ty we want to d sable/ emove funct ons p oh b ted o est cted. Rathe than say dent f ed n 3.4 6b ecommend p oh b ted o est cted n 3.4.6b. fo added cla ty. Fu the n fo m ng the assessment object ves fo th s fo low ng the ev 2 patte n, Po ts a e Rest cted, Funct ons a e est cted etc etc led to an assesso equ ement fo dent f cat on of all funct ons and a est ct on of some funct ons an dent f cat on of a l se v ces (as d st nct f om funct ons po ts and p otocols), and a block ng of some of those, etc. Go th ough that d ll and t y to b eak them all d ffe ently w thout, say, us ng blocked po ts to d sable a funct on o p otocol. You w l see that t s not only challeng ng, but an exe c se of t me and effo t that does not add to secu ty. Recommend n the fo mulat on of the AOs leav ng th s olled up athe than b eak ng down by each conjunct on as the b eak down fo assessment pu poses leads to a lot of effo t that does not p omote nfo mat on secu ty o the conf dent al ty of CUI.	Change to p oh b ted o est cted n 3.4.6b.
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		**895-922**	**3.4.8**	**Allow software by exception only. Recommend removal. Although CM-7(5) s now included in the Moderate baseline this is not a moderate control in commercial enterprise. Removal of the blacklist option for the control of software w ll represent an incredibly massive level of expenditure for implementation across commercial IT that is not set up to operate in this fashion. It will be equally challenging across large and small organizations although for d fferent reasons. This should be reserved for 172 implementation and not implemented n 171.**	Move to 172
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		940-957	3.4.10	System Component Invento y. The d scuss on sect on of th s adds eno mous equ ements that add noth ng to the conf dent al ty of CUI. Real ze that f you say the nvento y ncludes system components, and then system components = ha dwa e, softwa e, f mwa e, system name, softwa e owne s, softwa e ve s on numbe s, ha dwa e nvento y spec f cat ons (how s th s d ffe ent f om ha dwa e?), softwa e l cense nfo mat on, mach ne names (how s th s d ffe ent than system name?), netwo k add ess (how can I nclude IP add ess n the nvento y when they a e dynam ca ly allocated?) date of ece pt, cost, model, se al numbe , manufactu e , suppl e nfo mat on, component type, and phys cal locat on (so eve y t me an employee leaves wo k to go home, I have to update the locat on of the laptop n nvento y?). In l ne 950 nse t may between components and ncludes, as n effect ve accountab l ty of system components may nclude... Also, Invento y spec f cat ons **may** nclude... Othe w se you a e w t ng a equ ement fo DIB compan es to nvest n mass ve nvento y management capab l t es to cove each new spec f ed data type n a way that does noth ng to enhance the conf dent al ty of Fede al CUI.	Inse t may nclude
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		1016	3.5.2	Inse t the wo d can nto Systems use sha ed as n Systems can use sha ed... n o de to not seem to be mandat ng a pa t cula technology to meet the st ctu es of the cont ol. Fo example a small bus ness m ght meet th s cont ol w th phys cal secu ty cont ols. Only Bob has the key to oom w th the sma l se ve the bus ness uns and sto es the CUI. Bob v sually nspects Pauls compute to ensu e t s on h s autho zed nvento y l st befo e allow ng Paul nto the CUI oom that has the se ve . One poss ble scene o. I can also env s on othe token based equ ements o technolog es to p event dev ce connect on.	Inse t wo d can
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		1060	3.5.5	Inse t the wo d may as fo lows Cha acte st cs that may dent fy... You do not want to mandate n the d scuss on a equ ement to say dent fy a fo e gn nat onal fo eve y ema l add ess n the DIB. Fo mu t nat onal compan es who s the fo e gne ? Eve y US pe son wo k ng fo BAE needs to have FN n the ema l add ess? john-sm th.FN@bae.com? Eve y non US pe son wo k ng fo a US based D B cont acto must have FN n the ema l add ess? The ntent of the cont ol s to a low fo th s as an ODP. The d scuss on as w tten seems to walk that back and spec fy ce ta n data types that must be ncluded.	Inse t wo d may
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		1072-1073	3.5.7	You should not mandate the allowance of spaces and all p ntable cha acte s n passwo ds. Many legacy systems systems do not allow th s and t w ll cause a la ge amount of p oblems wh le not mean ngfully help ng secu ty. The except on p ocess fo cont acto s, unl ke the gove nment n accomodat ng legacy system equ ements s ve y ve y ve y d ff cu t to obta n. Effect vely mposs ble fo most. It would be bette fo secu ty and mo e mplementable to mandate a m n mum passwo d length, athe than a spec f c cha acte that must be allowable n a passwo d. An e ght cha acte passwo d, unfo tunately st ll the standa d fo many, w th a space, s st l an e ght cha acte passwo d. Recommend nse t ng nclud ng, whe e mplementable, spaces and all p ntable... I also ecommend cons de add ng a pa a fo m n passwo d length. 12-14 cha acte s at a m n. That s one that would add a lot of value to secu ty, s mplementable, and we need NISTs autho ty to sta t d v ng longe passwo ds. C yptog aph cally n mode n t mes 8 cha acte s s woefu ly nsuff c ent. Th s ecommendat on s a depa tu e f om ou no mal ecommendat ons of not spec fy ng how to mplement, howeve n th s case we feel wa anted based on the s gn f cant mpact to secu ty, and elat vely low cost to mplement. Th s change (spec fy a length not a complex ty equ ement) s cons stent w th NIST esea ch on how to best educe sk aga nst b ute fo ce passwo d attacks.	Remove equ ement fo nclud ng a space n passwo ds. Spec fy m n mum passwo d length.
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		1090	3.5.7	Inse t 'may' as n passwo ds may nclude n o de to not mandate that all elements must be p esent n all l sts	Inse t may
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		1123	3.5.12	On change default authent cato s p o to f st use. Th s may often not be poss ble. Passwo d. I ece ve a new oute . It has a default passwo d, Adm n. I must log n (f st use) w th the default passwo d n o de to change t to someth ng else. F om an assessment pe spect ve, how do I p ove no f st use of a default? Even when t s poss ble? If an authent cato s someth ng l ke a CAC ca d, how can I change t p o to f st use? B omet c. I cannot change my thumb p nt p o to f st use. The goal s not to deploy the oute w th the default passwo d st ll set. As wo ded though and when authent cato has been def ned to mean many d ffe ent th ngs, th s needs to be emoved, moved, o ewo ded. One poss ble app oach s the add t on of when poss ble. at the end of the sentence. Anothe would be to spec fy change a va able default athent cto set on a system o dev ce befo e use n a p otected system.	Inse t when poss ble o othe w se adjust language to allow fo authent cat on methods that cannot be changed p o to f st use.
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		1234	3.7.4	Recommend emove the wo d ma ntenance f om the l ne as n P event the emoval of equ pment conta n ng CUI So we do not want t to be just ma ntence equ pment that s p evented f om be ng emoved w thout be ng CUI checked but all equ pment.	Remove ma ntenance
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		1301	3.7.5	Inse t may nto Phys cally cont oll ng med a may nclude... othe w se the d scuss on could be nte p eted to mandate a se al zat on, cont ol, and check n and out of a l d g tal and non d g tal med a. So eve y p nted p ece of CUI pape would have to be numbe ed, ente ed nto the CUI nvento y, logged t acked etc. Note th s s a h ghe equ ement than appl ed to most class f ed nfo mat on and class f ed d g tal med a. Yes t needs to be locked, t needs to be labelled and cont o led, but def n ng cont ol as se al z ng and t ack ng eve y tem s above and beyond mode ate fo unclass f ed nfo mat on cons de ng that the USG does not mpose that equ ement on much mo e sens t ve class f ed nfo mat on.	Inse t may
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		1312-1315	3.8.2	Aga n the d scuss on sect on expands the equ ement to an nte p etat on that a l CUI med a must be se al zed and accounted fo nd v dually. Aga n th s s above and beyond the equ ements gene ally appl ed to class f ed med a and s not mode ate. Recommend add ng May nclude conduct ng nvento es, etc.	Inse t may
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		1320	3.8.3	Recommend add ng off s te befo e ma ntence. Techn ca ly as w tten th s says, San t ze system med a conta n ng CUI p o to ma ntence. So f the o gan zat ons autho zed CUI IT pe sonnel access a system med a th s lays a equ ement, ega dless of the status of be ng autho zed to v ew CUI, to san t ze the system. So f my laptop has an ssue, and IT s go ng to emotely access t to f x that ssue, the laptop must be san t zed f st. I eal ze that s not the ntent. That s what the cont ol says howeve . Recommend adjust ng the wo d ng to make t clea that th s s befo e access by pe sonnel who a e not autho zed fo CUI, t must be san t zed.	Inse t offs te

V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		1337	3.8.4	As w tten th s goes counte to the NARA gu del nes fo ma k ng system med a as conta ned n the NARA CUI ma k ng gu de, ve s on 1.1 Decembe 6 2016. It says spec f cally on page 23 Med a such as USB st cks, ha dd ves, and CD ROMs must be ma ked to ale t holde s to the p esenceof CUI sto ed on the dev ce. Due to space l m tat ons t may not be poss ble to nclude CUI Catego y, Subcatego y, o L m ted D ssem nat on Cont ol Ma k ngs. Recommend chang ng th s to Ma k system med a conta ng CUI n acco dance w th NARA o othe agency spec f c ma k ng gu dance. You m ght even ente ta n mak ng th s an ODP whe e NARA and DoD al eady have o gan zat onally spec f ed equ ements publ shed. NIST should not equ e ma k ngs ff t th N R	Recommend chang ng th s to Ma k system med a conta ng CUI n acco dance w th NARA o othe agency spec f c ma k ng gu dance.
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		1354	3.8.5	Th s emoves the capab l ty to p otect d g tal med a du ng t anspo t th ough phys cal p otect on mechan sms, fo example a locked conta ne . As w tten th s moves the 800-53 equ ement f om o gan zat onally def ned med a at est, to all med a unde go ng t anspo t. Recommend cont nu ng to a low secu e t anspo t w thout enc ypt on as an opt on. Ope at ona ly the e a e t mes when th s s equ ed pa t cula ly when mov ng f om a cont acto o gan zat on, to a gove nment o gan zat on whe e the gove nments st ct conf gu at on t l t ll f th l t t ll t t th t	Resto e opt on fo a te nat ve phys cal cont ols.
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		1400	3.8.9	The d scuss on sect on ma nta ns the o alte nat ve phys cal cont ols howeve the base secu ty equ ement only l sts c yptog aph c mechan sms. Recommend the add t on of o a te nat ve phys cal cont ols to the base equ ement.	Resto e opt on fo a te nat ve phys cal cont ols.
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		**1474-1491**	**3.10.1**	**What happens when there is no facility? In the modern cloud world, no company is start ng with on-prem systems. They are all cloud, and many in the current remote work environment have no corporate facilities at all, and are completely a cloud based system. How then can they issue authorization credentials for facility access? What f that facility only has a key, and not a badge reader? How are credentials created and ssued when they simply lock the front door? As written this looks at the problem completely through the big governments lens and not through the lens by which busines often operates. "Authorization credentials include ID badges, identificat on cards, and smart cards." This essentially mandates that every company in the DIB have a badge system of some kind. That does not match the effect ve secure operat on of small and medium sized businesses in many cases. Recommend mov ng this to an NFO.**	**Move to NFO**
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		1601	3.11.2	Inse t potent a ly nto when new vulne ab l t es potent ally affect ng the system a e dent f ed. If I al eady know the vulne ab l ty mpacts the system, I don t need to scan fo t.	Inse t potent ally
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		1620	3.11.2	Inse t should nto o gan zat ons should cons de	Inse t should
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		1632	3.11.2	Based on the 3.12.2 l ne 1685 comment, ecommend nse t ng n the d scuss on sect on as an add t onal pa ag aph, Vulne ab l ty emed at on should be t acked to dent fy all open vulne ab l t es, the sk status, and fo those unde go ng emed at on o m t gat on the t mel ne fo conduct ng that emed t on o m t gat on. Th s o s m l a language as a subst tute fo mandat ng that vulne ab l ty emed at on be t acked on the egulato y manadated POAM as outl ned n 3 11.4	Recommend nse t ng n the d scuss on sect on as an add t onal pa ag aph, Vulne ab l ty emed at on should be t acked to dent fy a l open vulne ab l t es, the sk status, and fo those unde go ng emed at on o m t gat on the t mel ne fo conduct ng that emed t on o m t gat on.
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		1638 -1652	3.11.4	Remove the language a ound POAM nse t on. Th s beg ns to d ect how an o gan zat on conducts the sk management p ocess and th nks solely about R sks as IT sks, and I suspect t comes f om a v s on that conflates sks and vulne ab l t es (they a e d ffe ent th ngs) that seems to es de n the cont ol f amewo k. F om a egulato y pe spect ve t also clutte s the use of the POAM as a mandated mechan sm fo eco d ng and t ack ng cont ol sho tfalls. All sks a e NOT cont ol sho tfa ls no a e they th ngs that can always be f xed o mplemented. Often the m t gat on s ongo ng fo eve . The sk ex sts. Supply cha n sk w l go on fo eve . I know of a numbe of o gan zat onal app oaches do ng a ve y good job of dent fy ng and m t gat ng sk, and the p ocesses do not nclude putt ng th ngs nto a POAM, yet they cont nue to t ack and m t gate those sks. Cu ently the a numbe of ways to add ess th s. Mandat ng nclus on n the POAM w ll cause ssues w th gove nance p ocesses b oadly n a way that does noth ng to dec ease the sk to the conf dent al ty of CUI.	Remove language a ound POAM nse t on.
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		1665-1666	3.12.1	and ensu e compl ance to vulne ab l ty m t gat on p ocedu es. Recommend emoval of th s ph ase. Vulne ab l ty m t gat on p ocedu es a e ust one of the 110 secu ty equ ements/cont ols. The e a e many and we al eady m x the vulne ab l ty management p ocess ac oss to many of them (I would p efe to see them t ghtly bundled but a la ge conve sat on that l kely st etches nto 800-53). Do vulne ab l ty management ght, and cove t n one place. Th s ph ase he e just mudd es wate s that a e al eady mu ky enough a ound th s top c.	Remove ph ase
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		1675-1677	3.12.1	O gan zat ons can choose to use othe types of assessment act v t es, such as vulne ab l ty scann ng and system mon to ng, to ma nta n the secu ty postu e of the system du ng the system l fe cycle. Recommend emov ng th s sentence. It mpl es that vul scann ng s a subst tute fo secu ty assessment and that s NOT the case. No s the amo phous system mon to ng a subst tute fo the equ ed secu ty assessment p ocess.	Remove sentence
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		1684	3.12.2	ewo d to be act ons to co ect weaknesses o def c enc es n cont ols Cont ol fa lu es can be dent f ed at t mes othe than cont ol assessments, l ke nc dent esponse. If you f nd a cont ol fa lu e ts co ect on should go on the POAM ega dless of whe e you found t.	ewo d to be act ons to co ect weaknesses o def c enc es n cont ols
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		1685	3.12.2	We note that th s s n the CA-5 cont ol, howeve ecommend the emoval of bullet 2. We cannot mandate the nclus on of a l vulne ab l t es dent f ed n the system n the POAM. Th ngs l ke the DoD mandat ng that assessments cannot sta t unt l all POAM tems a e closed as de, even fo a mode ate s zed o gan zat on at any g ven t me th s s l kely thousands of ent es. Fo la ge o gan zat ons potent al 10s of thousands. The vulne ab l ty management p ocess should not be fo ced to be conflated w th the cont ols management p ocess. Th s s deep n the weeds of how to and ecommend that NIST should st ck to what needs to be done to the max mum extent poss ble athe than p esc b ng that a l vulne ab l t es need to be managed on a compl ance mandated document w th compl ance mandated fo ms. Unde vulne ab l ty management, n the d scuss on mandate that vulne ab l t es must be t acked. We have added a ecommendat on at the app op ate l ne.	Remove bullet 2
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		1710	3.12.3	Add the sentence, Ident f ed cont ol fa lu es should be added to the POAM as nd cated n 3.12.2.	Add the sentence, Ident f ed cont ol fa lu es should be added to the POAM as nd cated n 3 12.2.
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		1733	3.12.6	Inse t CUI exchange n f ont of ag eements. So not a l ag eements but spec f cally CUI exchange ag eements.	Inse t CUI exchange n f ont of ag eements.
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		1782	3.13.1	Inse t may p o to ncludes fo systems may nclude… to p event an nte p etat on of mandat ng un ve sal mplementat on of the th ee l sted est ct ons	Inse t may p o to ncludes fo systems may nclude…
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		1788	3.13.1	Inse t should nto o gan zat ons should cons de	Inse t should nto o gan zat ons should cons de
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		**1867-1888**	**3.13.8**	**The theme seems to be to require encrypt on at rest for all CUI. Based on the "not in process or n transit" standard outlined at line 1879 some level of super encryption will be needed for a l CUI whereever present n the contractors system. This seems to be a significant uplift from the 800-53 moderate requirement which mitigates this with an ODP. So a scenerio. We receive a properly encrypted emailed CUI document from our government sponsor. We open and decrypt the email us ng our medium assurance token. After rev ewing the file we save it to our hard drive. On a laptop with b tlocker encryption enabled that would only encrypt when the device was shut down. Based on the not in process standard, it would seem to drive a need for an additional FIPS validated encryption method that would protect the CUI when not in process. Extend this scenerio to servers and databases. This will add massive complexity to the CUI handling process across the DIB and exceed the implemented standard in government networks for CUI documents. We recommend that this requ rement be reserved for certain types of CUI specified where needed and not be applied to a l CUI basic.**	**Restore a lowance for alternative physical controls**
V ncent Scott, Defense Cybe secu ty G oup	Gene al	Publ cat on		2001	3.14.1	Flaw Remed at on “b. Test softwa e and f mwa e updates elated to flaw emed at on fo effect veness and potent al s de effects befo e nstallat on” Th s does not d ectly mpact the conf dent al ty of CUI. S de effects a e not the p oblem of CUI conf dent al ty but of ava lab l ty of the system. Effect veness test ng s beyond the capab l ty of most comme c al bus nesses so the test ng that would be done could not mo e el ably dete m ne that fo example a ze o day has been effect vely patched than the test ng conducted by the vendo p oduc ng the patch. In tu n the delays fo test ng can eas ly, and do whe e they a e pe fo med, nc ease the sk fo conf dent al ty because t delays the nst lat on of needed patches. Th s equ ement w ll esu t n a net-negat ve secu ty fo bus nesses. Many bus nesses typ cally conf gu e the systems to accept and nstall vendo secu ty updates automat cally. Automat c patch ng esults n much qu cke flaw emed at on, wh ch s ve y mpo tant. The vast majo ty of bus ness IT depa tments a e less qual f ed than the t usted vendo s to test and f lte patches. Fo example, many compan es use M c osoft as one of the p ma y vendo s. M c osoft spends b l ons of do la s on cybe secu ty and the nte nal test and ev ew p ocess fo patch ng. Th s cont ol means we cannot accept push updates f om M c osoft, but nstead must conf gu e ou systems to REJECT patches unt l the nte nal IT depa tment manually packages them and pushes them to a test g oup, then to p oduct on. Fo a bus ness, th s 1) g eatly nc eases latency befo e patch ng f om ~12 hou s to 15-30 days, 2) equ es add ng ext a nf ast uctu e to manage the p ocess, such as a non-FedRAMP patch management solut on, wh ch nc eases the attack su face of the nfo mat on system, 3) nc eases IT bu den by at about many hou s pe week conduct ng test ng act v t es that a e less capable than those of the vendo n most cases. Fo a typ cal bus ness mplement ng th s equ ement, the p oposed benef t test ng patches to dete m ne f they a e mal c ous) s negl g ble. Unless an expl c t cont ol s added to th s effect, most bus ness IT depa tments w ll not pe fo m netwo k analys s o behav o analys s du ng test ng to dent fy mal c ous behav o . They w ll s mply slow down the patch ng p ocess d amat ca ly. **This change will result in a net negat ve for secur ty**. Fo most bus nesses, the sk of a t usted vendo be ng comp om sed and push ng a bad patch s less than the un ntended consequence of nc eas ng latency n flaw emed at on and nc eas ng attack su face.	Remove equ ement